



ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (Υ.Π.Δ / D.P.O)

ΑΠΟΣΤΟΛΟΣ ΖΙΩΖΙΑΣ
ΔΙΚΗΓΟΡΟΣ - ΔΙΑΜΕΣΟΛΑΒΗΤΗΣ

Υπεύθυνος Προστασίας Δεδομένων / DPO

Άρθρα 37-39

Η Ευρωπαϊκή Ένωση το έτος 2016 θέσπισε ένα νέο νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων, για την εφαρμογή του οποίου έχει επενδύσει ιδιαίτερα. Η εισαγωγή ενός νέου ανεξάρτητου θεσμού, του Υπεύθυνου Προστασίας Δεδομένων, ο ορισμός του οποίου είναι υποχρεωτικός για μεγάλες κατηγορίες οντοτήτων (υπηρεσιών, επιχειρήσεων, οργανισμών), καθολικά στον δημόσιο τομέα και σε σημαντικό βαθμό του ιδιωτικού τομέα, βρίσκεται στην κατεύθυνση της επιβολής της πραγματικής εφαρμογής του νέου αυτού θεσμικού πλαισίου.

Η έννοια του Υπευθύνου Προστασίας Δεδομένων δεν είναι καινούργια. Αν και η οδηγία 95/46/ΕΚ δεν επέβαλε σε κανέναν οργανισμό την υποχρέωση να ορίσει υπεύθυνο προστασίας δεδομένων, η συγκεκριμένη πρακτική αναπτύχθηκε σε αρκετά κράτη μέλη στο πέρασμα του χρόνου. Ο ΓΚΠΔ αναγνωρίζει τον Υπεύθυνο Προστασίας Δεδομένων ως καίρια συνιστώσα του νέου συστήματος διακυβέρνησης δεδομένων και θεσπίζει τις προϋποθέσεις για τον ορισμό, τη θέση και τα καθήκοντα του.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

υπεύθυνος επεξεργασίας & εκτελών την επεξεργασία ορίζουν υποχρεωτικά όταν:

- α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, (Εξαιρέση δικαστήρια στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας)
- β) **βασικές δραστηριότητες** απαιτούν τακτική & συστηματική παρακολούθηση υποκειμένων σε μεγάλη κλίμακα, ή
- γ) **βασικές δραστηριότητες μεγάλης κλίμακας** επεξεργασία ειδικών κατηγοριών ΔΠΧ (αρ.9) & δεδομένων ποινικές καταδίκες και αδικήματα (αρ.10)

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

υπεύθυνος επεξεργασίας & εκτελών την επεξεργασία ορίζουν υποχρεωτικά όταν (συνέχεια):

βασικές δραστηριότητες

- «οι καίριες πράξεις που είναι αναγκαίες για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία».
- δεν θα πρέπει, πάντως, να δίδεται ερμηνεία προς την κατεύθυνση της εξαίρεσης δραστηριοτήτων όταν η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

Παραδείγματα

- Νοσοκομείο: βασική δραστηριότητα είναι η παροχή υγειονομικής περίθαλψης. Όμως, δεν μπορεί να παρέχει υγειονομική περίθαλψη με ασφαλή και αποτελεσματικό τρόπο εάν δεν επεξεργάζεται ιατρικά δεδομένα (π.χ. ιατρικούς φακέλους ασθενών). Η επεξεργασία των εν λόγω δεδομένων θα πρέπει να θεωρείται, επομένως, ως μία από τις βασικές δραστηριότητες κάθε νοσοκομείου, **οφείλουν να ορίζουν ΥΠΔ.**
- Ιδιωτικές εταιρείες ασφαλείας: αναλαμβάνουν τη φύλαξη ιδιωτικών εμπορικών κέντρων και δημόσιων χώρων. Βασική δραστηριότητα η φύλαξη, η οποία είναι άρρηκτα συνδεδεμένη με την επεξεργασία ΔΠΧ, **οφείλουν να ορίσουν ΥΠΔ.**

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

Δραστηριότητες όπως π.χ.:

- η καταβολή μισθών στους υπαλλήλους του οργανισμού,
- η ανάπτυξη συνήθων δραστηριοτήτων υποστήριξης Τ.Π.,

είναι παραδείγματα αναγκαίων λειτουργιών υποστήριξης της βασικής δραστηριότητας ή του κύριου τομέα δραστηριότητας του οργανισμού. Μολονότι οι εν λόγω δραστηριότητες είναι αναγκαίες ή ουσιώδεις, θεωρούνται κατά κανόνα ως παρεπόμενες λειτουργίες του οργανισμού και όχι ως η βασική του δραστηριότητα.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

- Παραδείγματα επεξεργασίας δεδομένων ΣΕ μεγάλη κλίμακα:
 - ασθενών στο πλαίσιο της συνήθους λειτουργίας ενός νοσοκομείου,
 - πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρείας ή μιας τράπεζας,
 - προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης,
 - από παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου.
 - από εκπαιδευτικούς οργανισμούς.
 - από θρησκευτικούς οργανισμούς.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

Παραδείγματα που **ΔΕΝ** συνιστούν επεξεργασία δεδομένων μεγάλης κλίμακας:

- δεδομένων ασθενών από ιδιώτη ιατρό,
- δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

Παράδειγμα:

Κατασκευαστική εταιρεία μεσαίου μεγέθους αναθέτει υπερβολικά την παροχή υπηρεσιών επαγγελματικής υγείας σε εξωτερικό εκτελούντα την επεξεργασία, ο οποίος έχει πολλούς παρόμοιους πελάτες.

Ο εκτελών την επεξεργασία οφείλει να ορίσει υπεύθυνο προστασίας δεδομένων σύμφωνα με το άρθρο 37 παράγραφος 1 στοιχείο γ', εφόσον η επεξεργασία είναι μεγάλης κλίμακας.

Ο κατασκευαστής, αντίθετα, δεν βαρύνεται απαραίτητως με την υποχρέωση να ορίσει υπεύθυνο προστασίας δεδομένων.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

Ένας (1) μόνο Υπεύθυνος Προστασίας Δεδομένων (DPO) μπορεί να οριστεί:

- Όμιλος επιχειρήσεων (προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον DPO)
- Δημόσια αρχή ή Δημόσιος φορέας (λαμβάνεται υπόψη η οργανωτική τους δομή και το μέγεθός τους)
- Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

ΠΡΟΣΟΝΤΑ

Ο Υπεύθυνος Προστασίας Δεδομένων διορίζεται:

- βάσει επαγγελματικών προσόντων.
- βάσει εμπειρογνωσίας στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων.
- βάσει ικανότητας εκπλήρωσης των καθηκόντων (αρ 39).

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 37

ΘΕΣΗ στην ΕΤΑΙΡΕΙΑ:

- Μπορεί να είναι μέλος του προσωπικού.
- Ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.
- Τα στοιχεία επικοινωνίας του ανακοινώνονται στην εποπτική αρχή.

Θέση του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 38

Συμμετέχει, Δεόντως & Εγκαίρως ΣΕ ΟΛΑ τα ζητήματα σχετικά με προστασία ΔΠΧ

- να καλείται ο υπεύθυνος προστασίας δεδομένων να συμμετέχει τακτικά στις συσκέψεις στελεχών της διοίκησης.
- να είναι παρών όταν λαμβάνονται αποφάσεις που έχουν επιπτώσεις στην προστασία δεδομένων.
- να δίδεται πάντοτε η δέουσα βαρύτητα στη γνώμη του υπευθύνου προστασίας δεδομένων.
- να ζητείται απαραίτητως άμεσα η γνώμη του υπευθύνου προστασίας δεδομένων σε περίπτωση παραβίασης δεδομένων ή άλλου σχετικού συμβάντος.

Θέση του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 38

Ο υπεύθυνος επεξεργασίας & εκτελών στηρίζουν την άσκηση των καθηκόντων του Υπευθύνου Προστασίας Δεδομένων (αρ.39) παρέχοντας:

- i. απαραίτητους πόρους.
- ii. πρόσβαση σε δεδομένα & πράξεις επεξεργασίας.
- iii. πόρους απαραίτητους για διατήρηση εμπειρογνωσίας του.

Θέση του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 38

- Διασφαλίζεται ότι ΔΕΝ λαμβάνει εντολές για την άσκηση των καθηκόντων.
- ✓ Δεν απολύεται.
- ✓ Δεν υφίσταται κυρώσεις.
- ✓ Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο.
- Υποκείμενα μπορούν να επικοινωνούν για κάθε ζήτημα ΔΠΧ.
- Δεσμεύεται από τήρηση απορρήτου ή εμπιστευτικότητας.

Θέση του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρο 38

- Επιτελεί και άλλα καθήκοντα και υποχρεώσεις **MONO AN ΔΕΝ** συνεπάγονται σύγκρουση συμφερόντων.
- Θέσεις όπου εντοπίζονται συνήθως συγκρούσεις συμφερόντων:
 - ανώτερης διοίκησης:
 - διευθύνων σύμβουλος
 - οικονομικός διευθυντής
 - προϊστάμενος τμήματος μάρκετινγκ
 - προϊστάμενος ανθρωπίνων πόρων
 - προϊστάμενος τμήματος πληροφορικής
 - κατώτερων βαθμίδων:
 - εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας.

Καθήκοντα του υπευθύνου προστασίας δεδομένων

Άρθρο 39

τουλάχιστον :

1. ενημερώνει/συμβουλεύει υπεύθυνο επεξεργασίας ή εκτελούντα και υπαλλήλους για υποχρεώσεις.
2. παρακολουθεί συμμόρφωση με κανονισμό - άλλες διατάξεις Ένωσης ή κράτους μέλους, π.χ:
 - ανάθεση αρμοδιοτήτων
 - ευαισθητοποίηση
 - κατάρτιση των υπαλλήλων
 - ελέγχους.
3. συνεργάζεται με εποπτική αρχή.

Καθήκοντα του υπευθύνου προστασίας δεδομένων

Άρθρο 39

4. σημείο επικοινωνίας με αρχή/ πραγματοποιεί διαβουλεύσεις.

5. Λαμβάνει υπόψη τον κίνδυνο των πράξεων επεξεργασίας, συνεκτιμώντας:
 - φύση
 - πεδίο εφαρμογής
 - πλαίσιο
 - σκοπούς

Καθήκοντα του υπευθύνου προστασίας δεδομένων

Άρθρο 39

6. παρέχει συμβουλές για την εκτίμηση αντικτύπου και παρακολουθεί την υλοποίηση (αρ 35)
- εάν πρέπει ή όχι να διενεργήσει εκτίμηση αντικτύπου
 - ποια μεθοδολογία πρέπει να ακολουθήσει
 - τι εγγυήσεις (περιλαμβανομένων των τεχνικών και οργανωτικών μέτρων) πρέπει να εφαρμόσει
 - εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου και εάν τα συμπεράσματά είναι σύμφωνα με τον ΓΚΠΔ

Αν ο υπεύθυνος επεξεργασίας διαφωνεί με τις συμβουλές του ΥΠΔ., τότε στα έγγραφα της εκτίμησης αντικτύπου θα πρέπει να καταγραφούν γραπτώς οι λόγοι για τους οποίους δεν λήφθηκαν υπόψη οι συμβουλές.

Καθήκοντα του υπευθύνου προστασίας δεδομένων

Άρθρο 39

Αρχεία των δραστηριοτήτων επεξεργασίας

- ❖ Η τήρησή τους = **ευθύνη** του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία,

ΟΧΙ του DPO / υπευθύνου προστασίας δεδομένων.

- ❖ Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να αναθέτει στον ΥΠΔ το καθήκον να τηρεί τα αρχεία των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

Ορισμός του Υπευθύνου Προστασίας Δεδομένων / DPO

Άρθρα 37-39

Ο ΥΠΔ/DPO φέρει προσωπική ευθύνη για περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις προστασίας των δεδομένων ;

Όχι.

- Ο Υπεύθυνος Προστασίας Δεδομένων/DPO **ΔΕΝ** φέρει προσωπική ευθύνη για περιπτώσεις μη συμμόρφωσης.
- **Υπεύθυνος** να διασφαλίζει και να αποδεικνύει είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

CONTROLLED COLOR RANGE
COMPLETE RGB GAMMA
DYNAMIC TOLERANCE

Σας ευχαριστώ.