Συχνές ερωτήσεις απαντήσεις για τον Υπεύθυνο Προστασίας Δεδομένων (DPO)

σύμφωνα με τον ΓΚΠΔ (ΕΕ 2016/679 GDPR)

Υπεύθυνος επικοινωνίας
Μπρης Δημήτρης
Μαθηματικός . MSc στα Πληροφοριακά συστήματα
Τηλ.: 210.64.25.819 6944.810.572
www.e-dinet.gr info@e-dinet.gr

Εισαγωγή

Σύμφωνα με τα **Άρθρα 37,38 & 39** του κανονισμού (**ΓΚΠΔ 2016/679 GDPR**), η εταιρεία ή ο οργανισμός σας, είτε είναι υπεύθυνος επεξεργασίας είτε εκτελών την επεξεργασία, οφείλει να διορίσει ΥΠΔ εφόσον οι βασικές δραστηριότητες που ασκεί περιλαμβάνουν την επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή την τακτική και συστηματική παρακολούθηση σε μεγάλη κλίμακα φυσικών προσώπων. Εν προκειμένω, η παρακολούθηση της συμπεριφοράς φυσικών προσώπων περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης προφίλ στο διαδίκτυο, συμπεριλαμβανομένων των σκοπών της συμπεριφοριστικής διαφήμισης.

Οι δημόσιες διοικήσεις (*συμπεριλαμβανόμενων και των ΝΠΔΔ*) έχουν **πάντα** την **υποχρέωση** να διορίζουν ΥΠΔ (με εξαίρεση τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους ιδιότητα).

Ο ΥΠΔ μπορεί να είναι **μέλος** του **προσωπικού** του **οργανισμού** σας ή μπορεί να είναι εξωτερικός συνεργάτης με βάση σύμβαση παροχής υπηρεσιών. Ο ΥΠΔ μπορεί να είναι φυσικό πρόσωπο ή οργανισμός.

Να σημειωθεί, ότι παρόλο που δεν είναι υποχρεωτικός ο διορισμός DPO, α**ποτελεί καλή πρακτική απόδειξης συμμόρφωσης** (*ο διορισμός DPO*) σύμφωνα με τις απαιτήσεις του κανονισμού

Ο **Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει** τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και **μεσολαβεί** μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). **Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός)** και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 του ΓΚΠΔ).

Ακολουθούν απαντήσεις σε συνήθη ερωτήματα

Συχνές Ερωτήσεις

1. Ποιοι οργανισμοί πρέπει να ορίζουν DPO;

Ο ορισμός DPO είναι υποχρεωτικός όταν:

- Η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία). Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.
- Απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα (π.χ. ασφαλιστικές ή τραπεζικές υπηρεσίες, υπηρεσίες τηλεφωνίας ή διαδικτύου, παροχή υπηρεσιών ασφαλείας, όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, όπως για σκοπούς συμπεριφορικής διαφήμισης).
- Διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Για τον προσδιορισμό της μεγάλης κλίμακας επεξεργασίας πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκομένων υποκειμένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού, β) ο όγκος και το εύρος των δεδομένων, γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας, δ) η γεωγραφική έκταση της επεξεργασίας. 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.

2. Δεν υποχρεούμαι, αλλά επιθυμώ να ορίσω DPO στην επιχείρησή μου. Τι ισχύει σε αυτή την περίπτωση;

Κάθε οργανισμός μπορεί να ορίσει DPO. Ακόμη και στις περιπτώσεις που ο ορισμός DPO δεν είναι υποχρεωτικός, ενθαρρύνονται τέτοιου είδους εθελοντικές ενέργειες. Όταν ένας οργανισμός ορίζει DPO σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός (βλ. ερώτηση 5).

3. Μπορεί να οριστεί ένας DPO για περισσότερους φορείς ή οργανισμούς;

Ναι. 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.

4. Ποια είναι τα καθήκοντα του DPO;

Ο DPO προάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του οργανισμού ή φορέα. Τα ελάχιστα καθήκοντα του DPO είναι τα ακόλουθα:

- Να ενημερώνει και να συμβουλεύει τον οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

- Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της.
- Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.).
- Να συνεργάζεται με την εποπτική αρχή.

5. Ποιες είναι οι υποχρεώσεις του εργοδότη ενός DPO;

Ο εργοδότης υποχρεούται να δημοσιεύσει τα στοιχεία επικοινωνίας του DPO και να τα ανακοινώσει στην εποπτική αρχή. Επίσης, οφείλει να διασφαλίζει ότι ο DPO:

- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).
- Έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας
- Έχει στη διάθεσή του τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, οικονομικοί πόροι, υποδομές, συνεχής κατάρτιση).
- Εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
- Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη.
- Όταν ασκεί πρόσθετα καθήκοντα, αυτά να μην συνεπάγονται σύγκρουση συμφερόντων (π.χ. δεν μπορεί να κατέχει θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, όπως θέσεις ανώτερης διοίκησης).
- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

6. Ο DPO είναι υπάλληλος ή εξωτερικός συνεργάτης;

Είτε το ένα είτε το άλλο. Ο DPO μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (εξωτερικός συνεργάτης). Σε κάθε περίπτωση, μπορεί να συνεπικουρείται από ομάδα, εφόσον απαιτείται. Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην ΕΕ.

7. Τι επαγγελματικά προσόντα θα πρέπει να έχει ο DPO; Προβλέπεται σχετική πιστοποίηση;

Ο DPO διορίζεται ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων του. Το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία. Παράλληλα, ο

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

DPO πρέπει να έχει γνώση του τομέα δραστηριότητας του οργανισμού ή φορέα στον οποίο απασχολείται αλλά και των τεχνολογιών πληροφορίας και ασφάλειας των δεδομένων.

Για οποιαδήποτε απορία – διευκρίνιση, επικοινωνήστε μαζί μας:

Μπρης Δημήτρης
Μαθηματικός . MSc στα Πληροφοριακά συστήματα
Τηλ.: 210.64.25.819 6944.810.572
www.e-dinet.gr info@e-dinet.gr