Ο ρόλος και η ευθύνη του Data Protection Officer σύμφωνα με τον νέο Γενικό Κανονισμό Προσωπικών Δεδομένων

General Data Protection Regulation - Καν. (ΕΕ) 679/2016

Ιωάννης Ε. Γιαννακάκης, *Δικηγόρος, Νομικός Σύμβουλος Νότιας Ευρώπης Ομίλου G4S**

Στις 16 Απριλίου 2016 ψηφίσθηκε από το Ευρωπαϊκό Κοινοβούλιο ο Γενικός Κανονισμός Προσωπικών Δεδομένων, νομοθέτημα άμεσης εφαρμογής σε όλα τα κράτη μέλη της Ευρωπαϊκής Ενωσης, το οποίο θα τεθεί σε ισχύ μετά την παρέλευση της μεταβατικής περιόδου για την προσαρμογή των κρατών, δηλαδή στις 25 Μαΐου 2018. Το νομοθέτημα αυτό αλλάζει ριζικά το τοπίο στον χώρο της Προστασίας των Προσωπικών Δεδομένων επιβάλλοντας πρόσθετες υποχρεώσεις σε Υπεύθυνους Επεξεργασίας και Εκτελούντες την Επεξεργασία προσωπικών δεδομένων ανάμεσα στις οποίες είναι ο υποχρεωτικός διορισμός Data Protection Officer (σ.σ. θα διατηρήσω τον αγγλικό όρο, καθώς αποδίδει πληρέστερα την ουσία του συγκεκριμένου όρου).

Ήδη από τον Φεβρούαριο 2016 η Επιτροπή του άρθρου 29 (Article 29 Working Party), η οποία αποτελεί την εποπτεύουσα αρχή των εθνικών Αρχών Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Συμβουλευτικό Όργανο της Ευρωπαικής Επιτροπής, ανακοίνωσε ότι θα εκδώσει διευκρινιστικές οδηγίες σχετικά με τον ρόλο και την ευθύνη του Data Protection Officer, όπως αυτή προδιαγράφεται στα άθρα 37-39 του κανονισμού. Οι οδηγίες αυτές εκδόθηκαν στις 16 Δεκεμβρίου 2016 αποσαφήνιζοντας αρκετά - όχι όμως όλα τα - ερωτήματα αναφορικά με τον θεσμό που αποκτά νέα βαρύτητα μετά την εισαγωγή του κανονισμού.

* Ο Ιωάννης Ε. Γιαννακάκης είναι νομικός, εξειδικευμένος στον τομέα της προστασίας προσωπικών δεδομένων. Είναι Certified Information Privacy Professional/Europe και Certified Information Privacy Manager από τον International Association of Privacy Professionals (IAPP) και Certified GDPR/Foundation Consultant από το IT Governance κατά ISO 17024.

I. Βασικά σημεία της Διευκρινιστικής Οδηγίας

Τα βασικά σημεία της Διευκρινιστικής Οδηγίας της Επιτροπής του άρθρου 29 συνοψίζονται ως εξής:

1. Σε ποιες περιπτώσεις είναι υποχρεωτικός ο διορισμός του Υπεύθυνου Προσωπικών Δεδομένων (Data Protection Officer).

Ο κανονισμός προδιαγράφει τρεις βασικές κατηγορίες περιπτώσεων:

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:

i) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, ή

ii) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή

iii) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9, καθώς και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

(α) Οι διευκρινήσεις της Επιτροπής του άρθρου 29 εστιάζουν στη διασαφήνιση της έννοιας «βασικές δραστηριότητες» (Core Activities), οι οποίες περιγράφονται ως «αναπόσπαστο τμήμα της επίδιωξης των εταιρικών σκοπών του Υπευθύνου ή Εκτελούντος την Επεξεργασία, όπως για παράδειγμα οι δραστηριότητες παρακολούθησης μιας εταιρίας παροχής υπηρεσιών ασφαλείας, με τις οποίες ελέγχει/παρακολουθεί έναν δημόσιο ή ιδιωτικό χώρο, οι δραστηριότητες επεξεργασίας ιατρικών φακέλων ασθενών που νοσηλεύονται σε ένα νοσοκομείο, καθώς και οι δραστηριότητες επεξεργασίας προσωπικών δεδομένων υπαλλήλων από έναν εξωτερικό συνεργάτη που διαχειρίζεται τη μισθοδοσία του προσωπικού μιας εταιρίας.

(β) Στην έννοια «συστηματική» και «τακτική» Παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα (regular and systematic monitoring) εντάσσονται όλες οι μορφές on line παρακολούθησης, όπως για παράδειγμα η παρακολούθηση των μετακινήσεων του υποκειμένου (location tracking), η επεξεργασία που στοχεύει στον καθορισμό της καταναλωτικής συμπεριφοράς και συνηθειών του υποκειμένου για διαφημιστιούς σκοπούς (behavioral advertising), καθώς και ο καθορισμός του προφίλ του υποκειμένου με βάση συγκεκριμένα προσωπικά δεδομένα που αφορούν την καταναλωτική του ταυτότητα, τις προτιμήσεις του, την επισκεψιμότητα σε συγκεκριμένα καταστήματα (Profiling).

(γ) Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (των Ευαίσθητων Προσωπικών Δεδομένων της Οδηγίας 96/45) σε μεγάλη κλίμακα, όπως δεδομένων που αφορούν τη θρησκεία, τις πολιτικές πεποιθήσεις, τον σεξουαλικό προσανατολισμό, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, αλλά και γενετικα δεδομένων ή υλικό όπως και βιομετρικά στοιχεία τα οποία ορίζονται ως «Ειδικά Προσωπικά Δεδομένα» με τον Νέο Κανονισμό.

2. Η διευκρίνση της έννοια «επεξεργασίας σε μεγάλη κλίμακα» (Large Scale Processing) όμως παραμένει ασαφής και μάλλον αόριστη, καθώς τόσο το κείμε-

νο του κανονισμού όσο και οι οδηγίες της Επιτροπής Α29 δεν παραθέτουν αριθμητικά όρια για τον ορισμό της μεγάλης κλίμακας, αλλά γενικά παραδείγματα, όπως ασφαλιστικη εταιρία ή τράπεζα που επεξεργάζονται προσωπικά δεδομένων πελατών τους ή την επεξεργασία σε πραγματικό χρόνο των γεοτοπογραφικών δεδομένων (Geo_Location Data) πελατών μιας διεθνούς εταιρίας fast food για στατιστικούς σκοπούς.

3. Δημόσιοι Φορείς ή Αρχές, που ασχολούνται με την Υγεία, Τηλεπικονωνίες, Μεταφορές, ΔΕΚΟ κ.λπ. φαίνεται ότι θα υποχρεωθούν να διορίσουν Data Protection Officer. Το ίδιο και πολλές ιδιωτικές εταιρίες και οργανισμοί, συμπεριλαμβανομένων και μικρομεσαίων επιχειρήσεων, που επεξεργάζονται «Ειδικά Προσωπικά Δεδομένα» σε μεγάλη κλίμακα, όπως οι εταιρίες που διενεργούν κλινικές μελέτες (CRO's) και οι εταιρίες που διαχειρίζονται μισθοδοσία προσωπικού ή επεξεργάζονται καταναλωτικά προφίλ για κατηγορίες βασικών καταναλωτικών αγαθών.

4. Έρευνες που διενεργήθηκαν πανευρωπαϊκά, συμπέραναν ότι μόνο το 50% των επιχειρήσεων είναι έτοιμες να αντιμετώπισουν τα νέα δεδομένα που εισάγει ο Γενικός Κανονισμός, ενώ οι εκτιμήσεις των ειδικών προδιαγράφουν ανάγκη για διορισμό/δημιουργία θέσεων εργασίας για 28.000 (!!!!!!) Data Protection Officers σε πανευρωπαϊκό επίπεδο.

ΙΙ. Ένταξη του Data Protection Officer στην αγορά

1. Πώς θα ενταχθεί στην αγορά ο Data Protection Officer; Τι πρέπει να κάνουν οι επιχειρήσεις για να αποφύγουν τα βαρύτατα πρόστιμα που προβλέπει ο γενικός κανονισμός προσωπικών δεδομένων; Είναι έτοιμη η αγορά να αποδεχθεί τον θεσμικό ρόλο του Data Protection Officer όπως αυτός προδιαγράφεται στον κανονισμό; Δηλαδή ως ανεξάρτητο ειδικό στον χώρο των προσωπικών δεδομένων, με αποδεδειγμένη (πιστοποιημένη από ανεξάρτητο φορέα) γνώση και εμπειρία στη νομοθεσία και πρακτική εφαρμογή των Προσωπικών Δεδομένων, ο οποίος θα έχει εκέγγυα ανεξαρτησίας και θα αναφέρεται απευθείας στον CEO ή σε μέλος του Δ.Σ μιας εταιρίας; Θα ανατρέξουν οι εταιρίες στην «εύκολη» λύση της «εμβάπτισης» του εσωτερικού νομικού συμβούλου ή έμμισθου δικηγόρου σε Data Protection Officer ανεξάρτητα από το εάν ο τελευταίος έχει την ειδική γνώση και εμπειρία να αντιμετωπίσει την ευθύνη και τα καθήκοντα του θεσμικού αυτού ρόλου; Ή θα αντιμετώπισουν με τρόπο ουσιαστικό τις προκλήσεις και τις ανάγκες της νέας πραγματικότητας είτε εκπαιδεύοντας εσωτερικά τα στελέχη τους να λειτουργήσουν **αποκλειστικά** ως Data Protection Officers είτε προσλαμβάνοντας ανεξάρτητους επαγγελματίες, (με σύμβαση παροχής ανεξάρτητων υπηρεσιών ή με σύμβαση εξαρτημένης εργασίας, στην οποία όμως θα προδιαγράφεται σαφώς ο ρόλος και τα καθήκοντας του Data Protection Officer κατά τρόπο ώστε να αποφεύγεται η σύγκρουση συμφερόντων του τελευταίου, π.χ. εάν έχει παράλληλα καθήκοντα που αφορούν στην επεξεργασία προσωπικών δεδομένων στην εταιρία).

2. Οι οδηγίες της Επιτροπής του Ά29 διευκρίνησαν ότι ο Data Protection Officer, **δεν θα έχει προσωπική ευθύνη** στο πλαίσιο της άσκησης των καθηκόντων του, ότι περισσότερες εταιρίες ή όμιλοι εταιρειών που δραστηριοποιούνται σε διάφορα εδαφικά όρια μπορούν να διορίσουν έναν **κοινό** Data Protection Officer, αρκεί να μην ανακύπτει θέμα σύγκρουσης συμφερόντων του DPO, και ακόμα πως ο Data Protection Officer μπορεί να είναι ανεξάρτητος σύμβουλος μιας εταιρίας αρκεί να διασφαλίζονται οι προυποθέσεις που θέτει ο κανονισμός, δηλαδή η προσβασιμότητά του στα προσωπικά δεδομένα που τηρούνται στην επιχείρηση και η γνώση του αντικειμένου της επιχειρήσης, της εσωτερικής δομής και των πολιτικών της τελευταίας.

3. Ο ρόλος του Data Protection Officer, ως εξειδικευμένου, λειτουργικά ανεξάρτητου, στελέχους δεν περιορίζεται μόνο στην υποχρεωτική, κατά τον νέο κανονισμό, παρουσία του σε μια εταιρία με την έννοια της τυπικής πλήρωσης μιας θέσης εργασίας (tick box), όπως αντίστοιχα ο Ιατρός Εργασίας ή ο Τεχνικός Ασφαλείας. Ο Data Protection Officer αναλαμβάνει ουσιαστικά να εκπροσωπήσει την επιχείρηση έναντι των Αρχών, Εθνικών και Ευρωπαϊκών, να διασφαλίσει την εναρμόνιση της λειτουργίας της επιχείρησης σε ό,τι αφορά τις πολιτικές πρακτικές και τη μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με τον νέο αυστηρό νομοθετικό πλαίσιο και να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστίμων που προβλέπει ο κανονισμός τα οποία εκκινούν από 10.000.000 ευρώ ή το 2% του παγκόσμιου τζίρου, εάν πρόκειται για διεθνή όμιλο και φτάνουν σε περίπτωση παράβασης βασικών διατάξεων του κανονισμού σε 20.000.000 ευρώ ή στο 4% του παγκόσμιου τζίρου. Για να μπορέσουν οι επαγγελματίες του χώρου των προσωπικών δεδομένων να ανταποκριθούν στις αυξήμενες υποχρεώσεις και τη σοβαρότατη ευθύνη του ρόλου του Data Protection Officer απαιτείται η ουσιαστική επιμόρφωση και εκπαίδευσή τους, τόσο σε ό,τι αφορά τον Γενικό Κανονισμό Προσωπικών Δεδομένων, αλλά και σε ειδικά θέματα προσωπικών δεδομένων, όπως η κατάρτιση Data Privacy Impact Assessment (DPIA) σε περίπτωση εισαγωγής νέων υπηρεσιών ή προϊόντων που συνεπάγονται την επεξεργασία σε μεγάλη κλίμακα προσωπικών δεδομένων ή διαχειρίζονται ειδικά προσωπικά δεδομένα, η κατάρτιση ενός Προγράμματος/Πλαισίου Προσωπικών Δεδομένων εντός της Επιχείρησης/Εταιρίας, ο καθορισμός και η επικοινωνία Πολιτικής Προστασίας/Κανονισμού Προστασίας Προσωπικών Δεδομένων και η κοινοποίησή του στην Εθνική Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα και άλλα αντίστοιχα θέματα.

4. Ο Data Protection Officer θα πρέπει, κατά την άποψή μου, να λειτουργήσει ως επί κεφαλής ομάδας ειδικών (Task Force) που θα περιλαμβάνει ως μέλη του: IT, PR, Legal/Compliance και Information Security, δημιουργώντας έτσι μια εύελικτη ομάδα που θα αντιμετωπίσει επιτυχώς όλες τις προκλήσεις που θα ανακύψουν κατά την εφαρμογή του νέου αυστηρού νομοθετικου πλαισίου στον χώρο των προσωπικών δεδομένων· παράλληλα θα πρέπει να έχει άμεση πρόσβαση στη διοίκηση της εταιρίας ή των εταιριών που εκπροσωπεί. Σε αντίθετη περίπτωση υπάρχει σοβαρότατος κίνδυνος επιβολής εξοντωτικών για τις επιχειρήσεις διοικητικών προστίμων και, πέραν αυτών, κίνδυνος αναστολής της επεξεργασίας ή μεταφοράς συγκεκριμένων προσωπικών δεδομένων από τις εταιρίες που πρακτικά μπορεί να σημαίνει αναστολής της δραστηριότητας της επιχείρησης με τις αντίστοιχες συνέπειες.

5. Είναι αναγκαία η αφύπνιση και η δραστηριοποίηση της αγοράς, ώστε στον χρόνο που απομένει μέχρι την έναρξη ισχύος του Γενικού Κανονισμού να προετοιμασθεί κατάλληλα και επαρκώς για να αντιμετώπισει τα νέα δεδομένα, όπως επίσης είναι αναγκαίο οι επαγγελματίες των Προσωπικών Δεδομένων να επικαιροποιήσουν και εξειδικεύσουν τη γνώση τους, ώστε να μπορέσουν να αναλάβουν υπεύθυνα και ουσιαστικά τα καθήκοντα του Data Privacy Officer. Σ