

ΠΩΣ ΘΑ ΕΝΤΑΧΘΕΙ ΣΤΗΝ ΑΓΟΡΑ ΚΑΙ ΤΙ ΠΡΕΠΕΙ ΝΑ ΚΑΝΟΥΝ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΓΙΑ ΝΑ ΑΠΟΦΥΓΟΥΝ ΤΑ ΠΡΟ

Ο ρόλος και η ευθύνη του Data

Στις 16 Απριλίου 2016 ψηφίσθηκε από το Ευρωπαϊκό Κοινοβούλιο ο Γενικός Κανονισμός Προσωπικών Δεδομένων, νομοθέτημα άμεσης εφαρμογής σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης, 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 στο 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

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

Ι 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 αρίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:

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

β) οι βασικές δραστηριότητες του υπεύθυνου 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

γ) οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδικές και αδικήματα που αναφέρονται στο άρθρο 10.

Οι διευκρινίσεις της Επιτροπής του άρθρου 29 εστιάζουν στη διασαφήνιση της έννοιας «βασικές δραστηριότητες» (Core Activities) οι οποίες περιγράφονται ως «αναπόσπαστο τμήμα της επιδίωξης των εταιρικών σκοπών του υπεύθυνου ή εκτελούντος την επεξεργασία, όπως για παράδειγμα οι δραστηριότητες παρακολούθησης μιας εταιρείας παροχής υπηρεσιών ασφαλείας, με τις οποίες ελέγχει/παρακολουθεί ένα 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 εταιρείας.

Η έννοια «συστηματική» και «τακτική» παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα (regular and systematic monitoring) στην οποία εντάσσονται όλες οι μορφές on line παρακολού-

Έρευνες που διενεργήθηκαν πανευρωπαϊκά, συμπέραναν ότι μόνο το 50% των επιχειρήσεων είναι έτοιμες για να αντιμετωπίσουν 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 σύμφωνα με μελέτη του iapp σε πανευρωπαϊκό επίπεδο

θησης, όπως για παράδειγμα η παρακολούθηση των μετακινήσεων του υποκειμένου (location tracking), η επεξεργασία που στοχεύει στον καθορισμό της καταναλωτικής συμπεριφοράς και συνθηκών του υποκειμένου για διαφημιστικούς σκοπούς (behavioural advertising), καθώς και ο καθορισμός του προφίλ του υποκειμένου με βάση συγκεκριμένα προσωπικά δεδομένα που αφορούν την καταναλωτική του ταυτότητα, τις προτιμήσεις του, επισκεψιμότητα σε συγκεκριμένα καταστήματα (Profiling).

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (των ευαίσθητων προσωπικών δεδομένων της Οδηγίας 96/45) σε «μεγάλη κλίμακα», όπως δεδομένων που αφορούν θρησκεία, πολιτικές πεποιθήσεις, σεξουαλικό προσανατολισμό, συμμετοχή σε συνδικαλιστικές οργανώσεις αλλά και γενετικά δεδομένα ή υλικό όπως και βιομετρικά στοιχεία τα οποία ορίζονται ως «ειδικά προσωπικά δεδομένα» με το Νέο Κανονισμό.

II Η διευκρίνιση της έννοιας "επεξεργασία σε μεγάλη κλίμακα" (Large Scale Processing) ό-

συγκεκριμένου όρου). Ήδη από τον Φεβρουάριο 2016 η Επιτροπή του άρθρου 29 η οποία αποτελεί την εποπτεύουσα αρχή των εθνικών Αρχών Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Συμβουλευτικό Όργανο της Ευρωπαϊκής Επιτροπής ανακοίνωσε ότι θα εκδώσει διευκρινιστικές οδηγίες σχετικά με τον ρόλο και την ευθύνη του Data Protection Officer, όπως αυτή προδιαγράφεται στα άρθρα 37-39 του Κανονισμού.

Οι Οδηγίες αυτές εκδόθηκαν στις 16 Δεκεμβρίου 2016 αποσαφηνίζοντας αρκετά -όχι όμως όλα- ερωτήματα αναφορικά με τον θεσμό που αποκτά νέα βαρύτητα μετά την εισαγωγή του Κανονισμού.



μας παραμένει ασαφής και μάλλον αόριστη καθώς, τόσο το κείμενο του Κανονισμού όσο και οι Οδηγίες της Επιτροπής A29, δεν παραθέτουν αριθμητικά όρια για τον ορισμό της μεγάλης κλίμακας αλλά γενικά παραδείγματα, όπως ασφαλιστική εταιρεία ή τράπεζα που επεξεργάζονται προσωπικά δεδομένα πελάτη τους, ή την επεξεργασία σε πραγματικό χρόνο των γεο-τοπογραφικών δεδομένων (Geo _ Location Data) πελάτων μια διεθνούς εταιρείας fast food για στατιστικούς σκοπούς.

III Δημόσιοι φορείς ή αρχές, που ασχολούνται με την Υγεία, Τηλεπικοινωνίες, Μεταφορές, ΔΕΚΟ κ.λπ. φαίνεται ότι θα υποχρεωθούν να διορίσουν Data Protection Officer. Το ίδιο και πολλές ιδιωτικές εταιρείες και οργανισμοί, συμπεριλαμβανομένων και μικρομεσαίων επιχειρήσεων, που επεξεργάζονται «ειδικά προσωπικά δεδομένα» σε μεγάλη κλίμακα, όπως οι εταιρείες που διενεργούν κλινικές μελέτες (CRO's), οι εταιρείες που διαχειρίζονται μισθοδοσία προσωπικού ή επεξεργάζονται καταναλωτικά προφίλ για κατηγορίες βασικών καταναλωτικών αγαθών.

IV Έρευνες που διενεργήθηκαν πανευρωπαϊκά, συμπέραναν ότι μόνο το 50% των επιχειρήσεων είναι έτοιμες για να αντιμετωπίσουν 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 [HYPERLINK "https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/"](https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/) σύμφωνα με μελέτη του iapp σε πανευρωπαϊκό επίπεδο.

V Πώς θα ενταχθεί στην αγορά ο Data Protection Officer. Τι πρέπει να κάνουν οι επιχειρήσεις για να αποφύγουν τα βαρύτερα πρόστιμα που προβλέπει ο γενικός κανονισμός προσωπικών δεδομένων.

Είναι όμως 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

ΣΤΙΜΑ ΠΟΥ ΠΡΟΒΛΕΠΕΙ Ο ΚΑΝΟΝΙΣΜΟΣ

Data Protection Officer



Ο Ιωάννης Ε. Παννακάκης είναι νομικός, σύμβουλος Νότιας Ευρώπης του Ομίλου G4S, 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.

των προσωπικών δεδομένων, ο οποίος θα έχει εξέγχα ανεξαρτησίας και θα αναφέρεται απευθείας στον CEO ή σε μέλος του Δ.Σ. μιας εταιρείας;

Θα ανατρέξουν οι εταιρείες 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 αντιμετωπίσουν με τρόπο ουσιαστικό τις προκλήσεις και τις ανάγκες της νέας πραγματικότητας, είτε εκπαιδεύοντας εσωτερικά τα στελέχη τους, να λειτουργήσουν ΑΠΟΚΛΕΙΣΤΙΚΑ 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 καθήκοντα 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 εταιρεία);

VI Οι Οδηγίες της Επιτροπής του A29 διευκρινίζουν ότι ο Data Protection Officer, ΔΕΝ ΘΑ ΕΧΕΙ ΠΡΟΣΩΠΙΚΗ ΕΥΘΥΝΗ, στο πλαίσιο της άσκησης των καθηκόντων του, ότι περισσότερες εταιρείες ή όμιλοι εταιρειών που δραστηριοποιούνται σε διάφορα εδαφικά όρια, μπορούν να διορίσουν έναν ΚΟΙΝΟ 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 εταιρείας, αρκεί να διασφαλίζονται οι προϋποθέσεις που θέτει ο Κανονισμός, δηλαδή η προσβασιμότητά του στα προσωπικά δεδομένα που τηρούνται στην επιχείρηση και η γνώση του αντικειμένου της επιχείρησης, της εσωτερικής δομής και των πολιτικών της τελευταίας.

VII Ο ρόλος του Data Protection Officer, ως εξειδικευμένου, λειτουργικά ανεξάρτητου, στελέχους δεν περιορίζεται μόνο στην υποχρεωτική, κατά τον Νέο Κανονισμό, παρουσία του σε μία εταιρεία 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 εφαρμογή της λειτουργίας της επιχείρησης σε ό,τι αφορά στις πολιτικές πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς δεδομένων προσωπικού χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο και να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των σημαντικότερων και βαρύτερων 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 ή στο 4% του παγκόσμιου τζίρου.

Για να μπορέσουν οι επαγγελματίες του χώρου των προσωπικών δεδομένων να ανταποκριθούν στις αυξημένες υποχρεώσεις και τη σοβαρότατη ευθύνη του ρόλου του Data Protection Officer απαιτείται η ουσιαστική επιμόρφωση και εκπαίδευσή τους, τόσο σε ό,τι αφορά στον Γενικό Κανονισμό Προσωπικών Δεδομένων, αλλά και σε ειδικά θέ-

ματα 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, την κατάρτιση ενός προγράμματος/πλαισίου προσωπικών δεδομένων εντός της επιχείρησης/εταιρείας, ο καθορισμός και η επικοινωνία πολιτικής προστασίας/κανονισμού προστασίας προσωπικών δεδομένων και η κοινοποίησή του στην Εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και άλλα αντίστοιχα θέματα.

VIII Ο Data Protection Officer, θα πρέπει-κατά την άποψή μου- να λειτουργήσει ως επικεφαλής ομάδας ειδικών (Task Force) που θα περιλαμβάνει μέλη του IT, PR, Legal/ Compliance και Information Security δημιουργώντας μια ευέλικτη ομάδα που θα αντιμετωπίσει επιτυχώς όλες τις προκλήσεις που θα ανακύψουν κατά την εφαρμογή του νέου αυστηρού νομοθετικού πλαισίου στον χώρο των προσωπικών δεδομένων, και να έχει άμεση πρόσβαση στη διοίκηση της εταιρείας ή των εταιρειών που εκπροσωπεί. Σε αντίθετη περίπτωση, υπάρχει σοβαρότατος κίνδυνος επιβολής εξοντωτικών για τις επιχειρήσεις διοικητικών προστίμων, αλλά, πέραν αυτών, κίνδυνος αναστολής της επεξεργασίας ή μεταφοράς συγκεκριμένων προσωπικών δεδομένων από τις εταιρείες, που πρακτικά μπορεί να σημαίνει αναστολή της δραστηριότητας της επιχείρησης με τις αντίστοιχες συνέπειες.

IX 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 αντιμετωπίσει τα νέα δεδομένα, και στους επαγγελματίες των προσωπικών δεδομένων να επικαιροποιήσουν και εξειδικεύσουν τη γνώση τους ώστε να μπορέσουν να αναλάβουν υπεύθυνα και ουσιαστικά τα καθήκοντα του Data Protection Officer.