Εκπαίδευση, Δια Βίου Μάθηση, Έρευνα και Τεχνολογική Ανάπτυξη, Καινοτομία και Οικονομία

Τόμ. 2 (2019)

Πρακτικά του 2ου Πανελληνίου Επιστημονικού Συνεδρίου με Διεθνή Συμμετοχή «Ελλάδα-Ευρώπη 2020: Εκπαίδευση, Δια Βίου Μάθηση, Έρευνα, Νέες Τεχνολογίες, Καινοτομία και Οικονομία», Λαμία 28, 29, 30 Σεπτεμβρίου 2018

Ο κομβικός ρόλος και η συμβολή του Υπευθύνου Προστασίας Δεδομένων (DPO) στην επίτευξη της συμμόρφωσης με τον GDPR

Ευφροσύνη-Ειρήνη Δημουλά, Κωνσταντίνος Σιασιάκος

doi: 10.12681/elrie.1539

Ο κομβικός ρόλος και η συμβολή του Υπευθύνου Προστασίας Δεδομένων (DPO) στην επίτευξη της συμμόρφωσης με τον GDPR

Σιασιάκος Κωνσταντίνος[1], Δημουλά Ευφροσύνη – Ειρήνη[2]
k.siassiakos@asep.gr, sindylfh@hotmail.com
[1]PhD, ΑΣΕΠ, [2]MSc

Περίληψη

Η παρούσα εργασία περιγράφει τις αρμοδιότητες και τις ενέργειες του Υπευθύνου Προστασίας Δεδομένων (DPO), που εισάγει ο Γενικός Κανονισμός (GDPR) από τις 25 Μαΐου 2018, τόσο σε ευρωπαϊκό όσο κυρίως σε εθνικό επίπεδο. Αρχικά, λαμβάνοντας υπόψιν την παρουσία και τη δράση του στον ιδιωτικό και το δημόσιο τομέα αλλά και την ετοιμότητα συμμόρφωσης των επιχειρήσεων με τον GDPR, αναλύεται ο κρίσιμος ρόλος και τα απαιτούμενα προσόντα που θα πρέπει να διαθέτει, καθώς και οι προκλήσεις που καλείται να αντιμετωπίσει. Στη συνέχεια, τίθενται οι προβληματισμοί που δημιουργούνται ως προς τα καθήκοντα και το διορισμό του στις επιχειρήσεις, ενώ περιγράφεται η υπάρχουσα κατάσταση και τα προβλήματα ετοιμότητας και ελέγχου που αντιμετωπίζουν οι ιδιωτικοί αλλά και οι δημόσιοι φορείς στα πλαίσια του νέου Γενικού Κανονισμού. Στο τέλος, παρουσιάζονται τα κύρια συμπεράσματα της εργασίας, που μπορούν να αξιοποιηθούν για περαιτέρω προβληματισμό αλλά και κατανόηση του θεσμού το DPO από τις επιχειρήσεις και τους οργανισμούς.

Λέξεις κλειδιά: Υπεύθυνος Προστασίας Δεδομένων, Προσωπικά Δεδομένα, Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR), Έλεγχος Συμμόρφωσης.

Abstract

This paper describes the responsibilities and actions of the Data Protection Officer (DPO) introduced by the General Data Protection Regulation (GDPR) from May 25, 2018, both at European level and mainly at national level. Initially, by considering the DPO's presence and action in the private and public sector as well as the business readiness of compliance with GDPR, his crucial role and required skills are analyzed, as well as the challenges he faces. Subsequently, questions are raised about his duties and his recruitment in the enterprises, while the current situation and the problems of readiness and control, faced by private and public sector, are described in the framework of the GDPR. Finally, the main conclusions of the paper are presented, which can be used for further research and understanding of the DPO's role by enterprises and organizations.

Keywords: Data Protection Officer, Personal Data, General Data Protection Regulation (GDPR), Compliance Check.

1. Εισαγωγή

Η ραγδαία και συνεχής τεχνολογική εξέλιξη των τελευταίων ετών, κατέστησε αναγκαία τη θέσπιση ενός νέου ρυθμιστικού πλαισίου για την προστασία των προσωπικών δεδομένων, το οποίο θα διευρύνει τις ήδη υπάρχουσες μεθόδους προστασίας και θα διασφαλίζει ακόμα περισσότερο τα δικαιώματα των ατόμων.

Όλοι οι οργανισμοί που συλλέγουν, αποθηκεύουν και επεξεργάζονται δεδομένα ή συμπεριφορές σε μεγάλη κλίμακα ή είναι δημόσιες αρχές, καλούνται να ακολουθήσουν μία μακρά και αρκετά πολύπλοκη πορεία προς τη συμμόρφωσή τους με τις διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (EU 2016/679 - GDPR), στον πυρήνα του οποίου βρίσκεται ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (DPO).

Σύμφωνα με το κείμενο του Γενικού Κανονισμού (GDPR), η παρουσία και η δράση του κρίνεται απαραίτητη σε όλες τις επιχειρήσεις, ακόμη και στις μικρομεσαίες, οι οποίες μπορούν κατά διακριτική ευχέρεια να διορίσουν Υπεύθυνο Προστασίας Δεδομένων (DPO), είτε εσωτερικό είτε εξωτερικό, ο ρόλος του οποίου θα είναι κομβικός ως προς την υλοποίηση της συμμόρφωσης με το ισχύον κανονιστικό πλαίσιο.

2. Ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer-DPO)

2.1. Εισαγωγή

Ο Υπεύθυνος Προστασίας Δεδομένων δρα και ενεργεί σε καθεστώς ανεξαρτησίας και ανεξάρτητα από τον ειδικό νομικό χαρακτηρισμό της σύμβασης που τον συνδέει με τον εκάστοτε οργανισμό και από το αν ο οργανισμός αυτός λειτουργεί ως υπεύθυνος επεξεργασίας ή ως εκτελών την επεξεργασία. Πρακτικά διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων).

Ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός, ενώ δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση του οργανισμού με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον GDPR 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 GDPR). Το άρθρο 37 του Κανονισμού ορίζει το θεσμό του Υπευθύνου Προστασίας Δεδομένων ως υποχρεωτικό σε τρεις περιπτώσεις:

1. Όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,

2. Όταν 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, (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) ή

3. Όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 (π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία) και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο.

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.

Παραδείγματα εταιρειών που επιβάλλεται ο καθορισμός του DPO είναι οργανισμοί και επιχειρήσεις που δραστηριοποιούνται στον τομέα της Υγείας, των Τηλεπικοινωνιών, δημόσιοι φορείς και ΔΕΚΟ, οργανισμοί που επεξεργάζονται Ειδικά Προσωπικά Δεδομένα (π.χ. διαχείριση μισθοδοσίας, οικονομικά στοιχεία κ.ά.), κ.λπ. Το ίδιο και πολλές ιδιωτικές εταιρίες και οργανισμοί, συμπεριλαμβανομένων και μικρομεσαίων επιχειρήσεων, που επεξεργάζονται «ευαίσθητα προσωπικά δεδομένα» σε μεγάλη κλίμακα όπως οι εταιρίες που διενεργούν κλινικές μελέτες (CRO's).

Όσον αφορά τις δημόσιες αρχές, μπορεί να διοριστεί ένας ενιαίος Υπεύθυνος Προστασίας Δεδομένων σε μια ομάδα οργανώσεων. Ενώ δεν είναι υποχρεωτικό για τους οργανισμούς, εκτός των ανωτέρω, να ορίσουν έναν DPO, όλοι οι οργανισμοί θα χρειαστεί να εξασφαλίσουν ότι διαθέτουν τις δεξιότητες και το προσωπικό που απαιτείται ώστε να συμμορφώνεται με τη νομοθεσία του νέου Κανονισμού. Και η συμμόρφωση αυτή αποτελεί μία πολύπλοκη, πολυεπίπεδη και διατομεακή διαδικασία, που περιλαμβάνει πολλά στάδια, όπως ταξινόμηση δεδομένων, καταγεγραμμένες διαδικασίες συλλογής, ταξινόμησης, αποθήκευσης, μεταβίβασης και διαμοιρασμού δεδομένων, εκθέσεις αποτίμησης κινδύνου (DPIA), διαδικασίες αντιμετώπισης κινδύνων και άλλα. Η αδυναμία διορισμού ενός Υπεύθυνου Προστασίας Δεδομένων, σύμφωνα με τον GDPR, θα μπορούσε να οδηγήσει σε πρόστιμο.

2.2. Βασικές δραστηριότητες και καθήκοντα του DPO

Ο Υπεύθυνος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (DPO) είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον Κανονισμό και όλες τις σχετικές κανονιστικές απαιτήσεις και αποτελεί το πρώτο σημείο επίσημης επικοινωνίας του οργανισμού με την εποπτική αρχή, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για την Ελλάδα (ΑΠΔΠΧ), καθώς και με κάθε υποκείμενο που υπόκειται σε επεξεργασία προσωπικών δεδομένων από τον οργανισμό (εργαζόμενοι, πελάτες κ.λπ.). Η ευθύνη της μη συμμόρφωσης σύμφωνα με τις απαιτήσεις του Κανονισμού, αφορά το σύνολο του οργανισμού, συνεπώς ο DPO φέρει την ευθύνη να αποδεικνύει τη συμμόρφωση με τις απαιτήσεις του GDPR.

Επιπλέον, ο DPO οφείλει να προάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του οργανισμού ή φορέα, ενώ είναι αρμόδιος για:

-Να ενημερώνει και να παρέχει συμβουλές στον οργανισμό και στους υπαλλήλους του σχετικά με την εφαρμογή των απαιτήσεων και τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και από άλλες διατάξεις περί προστασίας δεδομένων.

-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, τήρηση των αρχείων καταγραφής).

-Να παρέχει συμβουλές για την εκτίμηση αντικτύπου (DPIA) και να παρακολουθεί την υλοποίησή της.

-Να συνεργάζεται με την εποπτική αρχή.

Τέλος, είναι ιδιαίτερα σημαντική η υποχρέωση του ως προς το επαγγελματικό απόρρητο που διέπει τη θέση του, καθώς σύμφωνα με το άρθρο 70 παρ. 5 του υπό διαβούλευση σχεδίου νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του GDPR, ο «υπεύθυνος προστασίας δεδομένων που παραβιάζει την υποχρέωση εχεμύθειας που τον βαρύνει στο πλαίσιο του επαγγελματικού απορρήτου ανακοινώνοντας ή αποκαλύπτοντας σε άλλον γεγονότα ή πληροφορίες που περιήλθαν σε γνώση του από τη θέση του κατά την εκτέλεση των καθηκόντων

του ή επ' ευκαιρία αυτών, με σκοπό να ωφεληθεί ο ίδιος ή τρίτος, ή για να βλάψει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ή το υποκείμενο των δεδομένων ή οποιονδήποτε τρίτο, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από δέκα χιλιάδες (10.000) ευρώ έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις».

2.3. Απαιτούμενα προσόντα και κριτήρια επιλογής ενός DPO

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 DPO πρέπει να έχει κατανοήσει εις βάθος τις απαιτήσεις του GDPR και να έχει γνώση και κατανόηση των δραστηριοτήτων που ενέχουν επεξεργασία δεδομένων στον οργανισμό που εκπροσωπεί, καθώς και των τεχνολογιών IT και των μεθόδων ασφαλείας πληροφοριών που εφαρμόζονται.

Η σημαντική του θέση στην εταιρεία, προϋποθέτει ακεραιότητα και επαγγελματικό ήθος τα οποία θα προάγουν την αναγκαιότητα της προστασίας προσωπικών δεδομένων εντός του οργανισμού. Ο ρόλος του στην οργανωτική δομή του οργανισμού θα πρέπει να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Δεν υπάρχουν καθορισμένα κριτήρια σχετικά με το ποιος πρέπει να είναι Υπεύθυνος Προστασίας Δεδομένων ή τι είδους προσόντα θα έπρεπε να έχει, αλλά σύμφωνα με τις κατευθηντήριες οδηγίες, θα πρέπει να διατίθεται νομοθεσία για την επαγγελματική πείρα και την προστασία των δεδομένων ανάλογα με το τι εκτελεί ο οργανισμός.

Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί επίσημα τα επαγγελματικά προσόντα και τις δεξιότητες ενός DPO, ενώ επίσης και ο GDPR, δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση.

3. Η συμβολή του DPO στην υλοποίηση της συμμόρφωσης με τον GDPR

3.1. Εισαγωγή

Συνίσταται, οι επιχειρήσεις και οι οργανισμοί να διορίσουν έναν «ηγέτη» στην πιλοτική διακυβέρνηση της προστασίας των δεδομένων εντός της δομής τους. Αυτό το άτομο θα εκτελεί εσωτερικά ενημερωτικές, συμβουλευτικές και ελεγκτικές εργασίες.

3.2. Διορισμός ενός Υπευθύνου Προστασίας Δεδομένων ("DPO")

Στα πλαίσια της εφαρμογής και συμμόρφωσης με τον GDPR, οι οργανισμοί μπορούν να διορίσουν έναν DPO, είτε εσωτερικό είτε εξωτερικό, που θα τους επιτρέψει να οργανωθούν καλύτερα. Παρ' όλο που ο ορισμός ενός DPO δεν είναι πάντοτε υποχρεωτικός, με βάση τις προϋποθέσεις που ορίστηκαν προηγουμένως, η παρουσία και η δράση του κρίνονται απαραίτητες σε όλες τις επιχειρήσεις, ακόμη και στις μικρομεσαίες, για τη διασφάλιση της συμμόρφωσης με τον GDPR.

Επιπλέον, προβλέπεται υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην εποπτική αρχή στοιχεία που αφορούν στον ορισμό του Υπευθύνου Προστασίας Δεδομένων.

Στο πλαίσιο αυτό η ΑΠΔΠΧ έχει αναρτήσει στην ιστοσελίδα της ειδικό έντυπο, το οποίο καλούνται να συμπληρώνουν και να αποστέλλουν οι υπεύθυνοι και εκτελούντες την επεξεργασία προκειμένου να ανακοινώσουν στην Αρχή τον ορισμό του υπευθύνου προστασίας σύμφωνα με την

προαναφερθείσα υποχρέωσή τους. Ο ορισμός του DPO ικανοποιείται μόνο με την υποβολή του συγκεκριμένου εντύπου, ενώ οποιαδήποτε προηγούμενη (πριν την 25η Μαΐου 2018) δήλωση στοιχείων υπευθύνου προστασίας δεδομένων που έχει υποβληθεί στην Αρχή δεν λαμβάνεται υπόψη.

Τέλος, ορίζεται ρητά ότι τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας Δεδομένων πρέπει να δημοσιοποιούνται προκειμένου να διασφαλίζεται η απρόσκοπτη επικοινωνία με τα υποκείμενα των δεδομένων.

Μόλις οι επιχειρήσεις ορίσουν έναν «πιλοτικό» υπεύθυνο για την εφαρμογή των μέτρων συμμόρφωσης με τον Κανονισμό και του παρέχουν ανθρώπινα και οικονομικά μέσα για να εκτελέσει τα καθήκοντά του, ολοκληρώνεται το πρώτο βήμα της συμμόρφωσης του οργανισμού με τον GDPR.

3.3. Ο κρίσιμος ρόλος του DPO

Ο ρόλος του στο εσωτερικό μίας επιχείρησης, ανεξαρτήτως του μεγέθους αυτής, μπορεί να συμβάλλει αποφασιστικά στην ενδυνάμωση της συμμόρφωσής της, η ύπαρξη της οποίας αποτελεί σήμερα σημαντικό ανταγωνιστικό πλεονέκτημα στην αγορά έναντι άλλων επιχειρήσεων.

1. Ο DPO πρέπει να συμμετέχει ενεργά σε όλα τα ζητήματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, ενώ η επιχείρηση θα πρέπει να διασφαλίζει αντιστοίχως την πρόσβαση του σε κάθε απαραίτητη για τον σκοπό αυτό πληροφορία σχετικά με προσωπικά δεδομένα και τις διαδικασίες επεξεργασίας τους.
2. Ο DPO πρέπει να έχει την αμέριστη υποστήριξη της επιχείρησης η οποία οφείλει να τον εφοδιάζει με όλα τα απαραίτητα μέσα για την επιτυχή εκπλήρωση των αρμοδιοτήτων του.
3. Ο DPO πρέπει να είναι σε θέση να δρα και να λειτουργεί αυτόνομα στο εσωτερικό της επιχείρησης.
4. Σε καμία περίπτωση δεν θα πρέπει ο ρόλος του DPO και η συνέπεια προς αυτόν να επιφέρει την τιμωρία του τελευταίου ή την απαλλαγή του εκ των καθηκόντων του εκ μέρους του υπευθύνου ή του εκτελούντος την επεξεργασία.
5. Η επιχείρηση οφείλει να μην αναθέτει στον DPO καθήκοντα τα οποία ενδέχεται να συγκρούονται με εκείνα τα οποία ο ίδιος έχει αναλάβει ως Υπεύθυνος Προστασίας Δεδομένων (π.χ. καθήκοντα θέσης Οικονομικού Διευθυντή, Διευθυντή τμήματος HR, Ιατρικού Διευθυντή κ.λπ)
6. Ο DPO μπορεί να συμβάλλει δυναμικά στην καταγραφή και τήρηση αρχείου αναφορικά με τις διαδικασίες επεξεργασίας που λαμβάνουν χώρα εντός της επιχείρησης, σύμφωνα πάντα με τις πληροφορίες που θέτουν υπόψιν τους ο υπεύθυνος ή ο εκτελών την επεξεργασία. Με αυτόν τον τρόπο μπορεί να ενδυναμωθεί η συμμόρφωση της επιχείρησης μέσω της συχνής πληροφόρησης και αναφοράς στον DPO.

Ένα ισχυρό πρόγραμμα συμμόρφωσης με τον GDPR, εποπτευόμενο από έναν κατάλληλο DPO μπορεί να συμβάλει στην ελαχιστοποίηση του κινδύνου παραβίασης προσωπικών δεδομένων και συνεπώς στην αποφυγή προστίμων και λοιπών κυρώσεων και αξιώσεων αποζημίωσης από τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης των δεδομένων τους. Μπορεί, τέλος, να ενισχύσει την αφοσίωση του προσωπικού της εταιρείας που το υιοθετεί, καθώς επίσης και τη φήμη και την αξιοπιστία της, βοηθώντας την να κερδίσει νέες ευκαιρίες.

3.4. Προκλήσεις που καλείται να αντιμετωπίσει ο DPO

Ο GDPR καθιστά σαφές ότι βασικός υπόχρεος συμμόρφωσης προς το συγκεκριμένο κανονιστικό πλαίσιο είναι όχι ο DPO αλλά ο ίδιος ο Υπεύθυνος Επεξεργασίας, ο οποίος και καλείται να εφαρμόσει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να είναι σε θέση να

αποδείξει ότι η επεξεργασία προσωπικών δεδομένων λαμβάνει χώρα σε συμμόρφωση με τις επιταγές του Κανονισμού. Αναδεικνύεται, έτσι, ένα ιδιαιτέρως σημαντικό ζήτημα, ήτοι ότι η συμμόρφωση προς το κανονιστικό πλαίσιο για την προστασία προσωπικών δεδομένων αποτελεί πρωταρχική εταιρική ευθύνη του ίδιου του υπευθύνου επεξεργασίας και όχι του DPO.

Ωστόσο, ο ρόλος του τελευταίου στο εσωτερικό μίας επιχείρησης θα αποτελέσει προϋπόθεση επίτευξης ενός υψηλού επιπέδου συμμόρφωσης, γεγονός που, αν μη τι άλλο, τον καθιστά αδιαμφισβήτητα απαραίτητο αλλά και αντιμέτωπο με μια σειρά προκλήσεων όπως:

- Να εκπροσωπήσει την Επιχείρηση έναντι των Αρχών, Εθνικών και Ευρωπαϊκών, ως διαμεσολαβητής.
- Να διασφαλίσει την εναρμόνιση της λειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές πρακτικές και τις μεθοδολογίες επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο.
- Να δημιουργήσει την κατάλληλη κουλτούρα στο ανθρώπινο δυναμικό της εταιρείας.
- Να εκπαιδεύσει το προσωπικό σχετικά με τις σημαντικές απαιτήσεις συμμόρφωσης του GDPR, την επεξεργασία δεδομένων και τη διενέργεια τακτικών ελέγχων ασφάλειας.
- Να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των βαρύτατων διοικητικών προστίμων που προβλέπει ο Κανονισμός, τα οποία ξεκινούν από 10 εκατομμύρια ευρώ ή στο 2% του παγκόσμιου τζίρου εάν πρόκειται για διεθνή όμιλο και φτάνουν σε περίπτωση παράβασης βασικών διατάξεων του Κανονισμού στα 20 εκατομμύρια ευρώ ή στο 4% του παγκόσμιου τζίρου.

Επιπλέον, ο DPO θα πρέπει να έχει τις κατάλληλες γνώσεις και δεξιότητες για να ανταποκριθεί στον ρόλο του, με αποδεδειγμένη (πιστοποιημένη από ανεξάρτητο φορέα) γνώση και εμπειρία στη νομοθεσία και πρακτική εφαρμογή των διαδικασιών διαχείρισης προσωπικών δεδομένων. Ακόμα θα έχει εχέγγυα ανεξαρτησίας και θα αναφέρεται απευθείας στον Διευθυντή ή σε μέλος του Διοικητικού Συμβουλίου (Δ.Σ.) της εταιρείας.

3.5. Προβληματισμοί σχετικά με το διορισμό ενός DPO

Λόγω της εμβέλειας του GDPR και εκτός Ευρωπαϊκής Ένωσης, πολλές εταιρείες θα πρέπει να ξοδεύουν χρήματα είτε σε έναν εσωτερικό DPO είτε σε έναν τρίτο φορέα, όπως μια δικηγορική εταιρεία ή μια επιχείρηση πληροφορικής που θα ενεργεί ως εξωτερικός Υπεύθυνος Προστασίας Δεδομένων. Σύμφωνα με μελέτες, περισσότεροι από 28.000 νέοι Υπεύθυνοι Προστασίας Δεδομένων πρέπει να προσληφθούν μέχρι το 2018, και αυτό ισχύει μόνο στην ΕΕ και στις Η.Π.Α. Σε παγκόσμιο επίπεδο όμως, ο αριθμός αυξάνεται στους 75.000. Με την έλλειψη λοιπόν ατόμων που εκπαιδεύονται στη διαχείριση των ευθυνών του DPO, είναι πιθανό ότι πολλές επιχειρήσεις θα αναζητήσουν την πρόσληψη ενός εξωτερικού DPO τρίτου.

Ωστόσο, πριν από την πρόσληψη ενός εξωτερικού DPO, οι επιχειρήσεις πρέπει να εξετάσουν τα ακόλουθα θέματα:

1. Δικαιολογείται το κόστος πρόσληψης ενός DPO με τη συμμετοχή του στο πρόγραμμα προστασίας προσωπικών δεδομένων μιας επιχείρησης;

Τα καθήκοντα του DPO δεν αφορούν μόνο την αντιμετώπιση καταστάσεων παραβίασης και τη συνεργασία με τις εποπτικές αρχές αλλά περιλαμβάνουν και αρμοδιότητες όπως την παρακολούθηση της συμμόρφωσης της επιχείρησης με τον GDPR, την παροχή συμβουλών κατά τη διενέργεια εκτιμήσεων αντικτύπου προστασίας δεδομένων και την ενημέρωση της επιχείρησης και των εργαζομένων της για υποχρεώσεις προστασίας δεδομένων. Επιπλέον, ένας DPO πρέπει να συμμετέχει τακτικά σε συνεδριάσεις με ανώτερα και μεσαία στελέχη και πρέπει επίσης να είναι εύκολα προσβάσιμος εντός του οργανισμού. Οι δικηγορικές εταιρίες και οι εταιρείες παροχής

συμβούλων πληροφορικής είτε χρεώνουν ανά ώρα είτε έχουν σταθερή τιμή για να παρέχουν τις υπηρεσίες τους. Έτσι, είναι σημαντικό να ληφθεί υπόψιν ότι ορισμένες ευθύνες, όπως η παρακολούθηση συναντήσεων και η παρακολούθηση της συμμόρφωσης της επιχείρησης με τον GDPR, μπορεί να είναι εξαιρετικά χρονοβόρες και δαπανηρές ανά ώρα. Ορισμένες εταιρείες παροχής υπηρεσιών δημιούργησαν μια πολιτική σταθερού ποσού που μπορεί να προσφέρει εξοικονόμηση κόστους, αλλά με κίνδυνο να θυσιάσει την ποιότητα, θέτοντας λιγότερο εξειδικευμένα και έμπειρα άτομα σε ρόλους DPO. Συνεπώς, σε μια ωριαία αμοιβή ή μισθολογική συμφωνία, μια επιχείρηση θα πρέπει να εξετάσει τις υπηρεσίες που περιλαμβάνονται συγκριτικά με την εμπειρία των ατόμων που θα εκτελούν αυτές τις υπηρεσίες.

2. Μπορεί ο πάροχος υπηρεσιών να ενεργεί ανεξάρτητα κατά την εκτέλεση των καθηκόντων του ως DPO;

Σύμφωνα με τις κατευθυντήριες γραμμές του GDPR του άρθρου 38 παράγραφος 3 και του άρθρου 29, ο DPO πρέπει να εκτελεί τα καθήκοντά του με ανεξάρτητο και αδιάβλητο τρόπο, δηλαδή δεν πρέπει να ενημερώνεται σχετικά με τον τρόπο αντιμετώπισης ενός θέματος και δεν μπορεί να του δοθεί εντολή να λάβει θέση σχετικά με το θέμα της προστασίας της ιδιωτικής ζωής των υποκειμένων. Ωστόσο, αυτό θα μπορούσε να αποτελεί ένα πιθανό πρόβλημα, ειδικά εάν ο πάροχος υπηρεσιών έχει πολλές δεσμεύσεις με την εν λόγω επιχείρηση. Εάν μια επιχείρηση έχει στενή σχέση με τον πάροχο υπηρεσιών, η γραμμή μπορεί να είναι πολύ «λεπτή» και μπορεί να οδηγήσει σε περιπτώσεις όπου μπορεί να ζητηθεί ή να ασκηθεί πίεση στον πάροχο υπηρεσιών να λάβει θέση με οποιονδήποτε τρόπο.

3. Έχει ο DPO άλλες δεσμεύσεις σχετικά με την προστασία της ιδιωτικής ζωής, την ασφάλεια των δεδομένων ή τις σχετικές με την πληροφορική τεχνογνωσίες με την επιχείρηση, οι οποίες θα μπορούσαν ενδεχομένως να δημιουργήσουν σύγκρουση συμφερόντων;

Σύμφωνα με τις κατευθυντήριες γραμμές του GDPR του άρθρου 38 παράγραφος 6 και του άρθρου 29, επιτρέπεται στον DPO να εκπληρώνει άλλα καθήκοντα, τα οποία όμως να μην οδηγούν σε σύγκρουση συμφερόντων με τα καθήκοντά του όσον αφορά τη θέση του σαν DPO. Για πολλές εταιρείες παροχής υπηρεσιών, αυτό μπορεί να αποτελεί πρόβλημα, ειδικά εάν είχαν συνεργαστεί με τη διοίκηση της επιχείρησης και κατά το σχεδιασμό του προγράμματος προστασίας προσωπικών δεδομένων της ή τη βοήθησαν να ερμηνεύσει τους κανόνες και τους κανονισμούς απορρήτου. Οι πάροχοι υπηρεσιών ενδέχεται να αισθάνονται άβολα όταν κάνουν διαπιστώσεις που αντιβαίνουν στις συμβουλές που παρείχαν σε προηγούμενη δέσμευση.

Συνεπώς ερωτήματα που θα πρέπει να εξετάζει μια επιχείρηση πριν τον διορισμό ενός εξωτερικού Υπευθύνου Προστασίας Δεδομένων είναι:

- Τι είδους σύμβαση αμοιβής προσφέρει ο εξωτερικός DPO;
- Εάν το ποσό αμοιβής είναι σταθερό: είναι οι παρεχόμενες υπηρεσίες επαρκείς για την επιχείρηση; Είναι κατάλληλα τα άτομα που χειρίζονται τα καθήκοντα ως DPO;
- Εάν το ποσό αμοιβής είναι ανά ώρα: είναι οι τιμές ανάλογες της εμπειρίας των ατόμων που εκτελούν καθήκοντα DPO; Υπάρχουν δυνατότητες έκπτωσης στην τιμή σε περίπτωση προκαταβολής του ποσού; Τι είδους καθήκοντα αναμένει η επιχείρηση να εκτελεί ο DPO;
- Ο DPO εκπροσωπεί και άλλες επιχειρήσεις στον ίδιο κλάδο;
- Η επιχείρηση έχει στενή σχέση με τον εξωτερικό DPO σε σημείο που μπορεί να προκαλέσει προβλήματα ανεξαρτησίας;
- Έχει ο εξωτερικός DPO εμπλακεί στο παρελθόν σε οποιαδήποτε εργασία προστασίας προσωπικών δεδομένων για την επιχείρηση; Μπορεί το έργο αυτό να προκαλέσει σύγκρουση συμφερόντων;

4. Η παρούσα κατάσταση στον ιδιωτικό και στο δημόσιο τομέα

4.1. Εισαγωγή

Η τωρινή εικόνα στην Ελλάδα, δείχνει ότι ειναι ολοσχερής η απουσία προετοιμασίας στη χώρα μας για την εφαρμογή του GDPR. Σύμφωνα με όλες τις ενδείξεις, η 25η Μαΐου 2018, τελική ημερομηνία εφαρμογής του Κανονισμού έβρισκε την Ελλάδα μεταξύ των οκτώ κρατών-μελών που δεν είχαν εναρμονίσει την εθνική με τη νέα κοινοτική νομοθεσία.

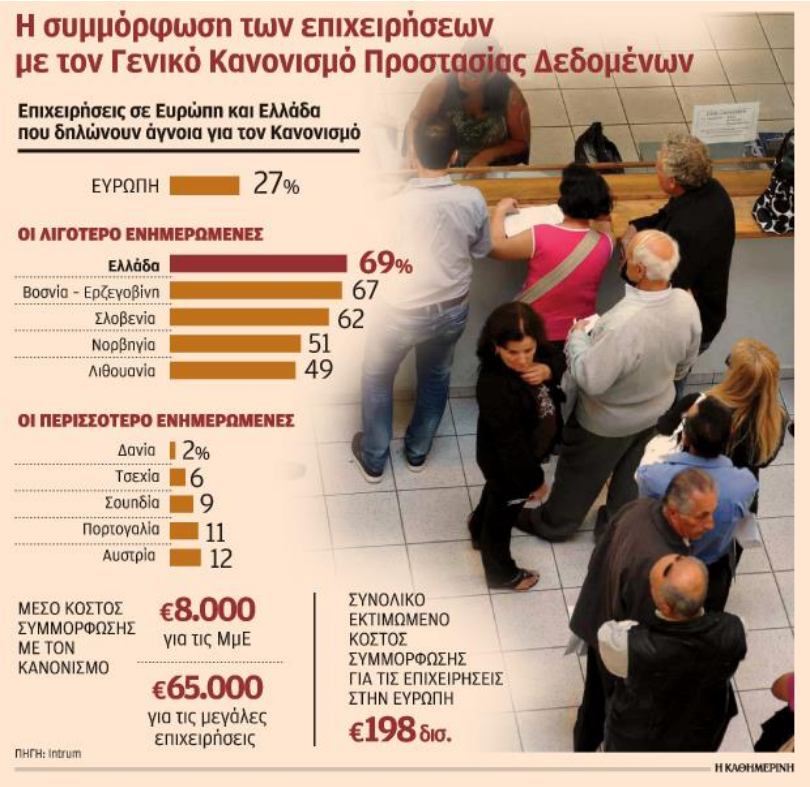
Αν και η νομοπαρασκευαστική επιτροπή που είχε οριστεί για τον σκοπό αυτό από το Υπουργείο Δικαιοσύνης ολοκλήρωσε το έργο της από τον περασμένο Μάρτιο, το σχετικό νομοσχέδιο, το οποίο, μάλιστα, είχε τεθεί και σε δημόσια διαβούλευση, δεν έχει εισαχθεί προς ψήφιση στη Βουλή. Στην πραγματικότητα, η αναγκαιότητα εναρμόνισης του θεσμικού πλαισίου της χώρας για το σύνολο των ανεξάρτητων αρχών της χώρας είναι αυτή που έχει καθυστερήσει τη διαδικασία ψήφισης του νομοσχεδίου, καθώς αναμένεται μια ολιστική προσέγγιση του θέματός τους. Το αποτέλεσμα είναι ότι ούτε ο νέος GDPR υιοθετείται αλλά ούτε και ο εκσυγχρονισμός του θεσμικού πλαισίου των ανεξάρτητων αρχών προωθείται. Σημειώνεται ότι την αρμοδιότητα για την εφαρμογή του κανονισμού έχει η ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

4.2. Ο DPO στον ιδιωτικό τομέα

Οι οντότητες του ιδιωτικού τομέα, όπως επιχειρήσεις, αλλά και ΜΚΟ, σύλλογοι, σωματεία, αστικές μη κερδοσκοπικές εταιρίες, συνεταιρισμοί, κοινοπραξίες κλπ, που είτε διεξάγουν τακτική και συστηματική παρακολούθηση είτε επεξεργάζονται ευαίσθητα δεδομένα σε μεγάλη κλίμακα και απασχολούν πάνω από 250 εργαζομένους, υποχρεούνται να ορίσουν DPO.

Έτσι, DPO υποχρεούνται να διαθέτουν ενδεικτικά:

- τα νοσοκομεία, οι κλινικές και άλλοι πάροχοι ιδιωτικών υπηρεσιών υγείας που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ασθενών (δε θα ισχύει για ιδιώτες ιατρούς ή άλλους επαγγελματίες υγείας σε επίπεδο ιδιωτικού ιατρείου),
- οι εταιρίες που παρέχουν υπηρεσίες φύλαξης ή διεξάγουν παρακολούθηση για λόγους ασφαλείας (εταιρίες security) ή και οι ίδιες οι επιχειρήσεις που διεξάγουν παρακολούθηση (πχ μέσω κλειστού κυκλώματος τηλεόρασης στις εγκαταστάσεις ή τα καταστήματά τους),
- οι επιχειρήσεις μηχανοργάνωσης ή διαχείρισης μισθοδοσίας για λογαριασμό άλλων επιχειρήσεων,
- οι εταιρίες κινητής και σταθερής τηλεφωνίας και υπηρεσιών ίντερνετ,
- οι ασφαλιστικές εταιρίες,
- οι τράπεζες,
- οι ιδιωτικές εταιρίες διαχείρισης μέσων μεταφοράς,
- κάθε επιχείρηση που συλλέγει δεδομένα των συναλλασσομένων με αυτή και τα χρησιμοποιεί για την κατασκευή «προφίλ» που αποκαλύπτουν τις προσωπικές προτιμήσεις, την ιδεολογία ή την καταναλωτική συμπεριφορά,
- κάθε επιχείρηση που συλέγει και χρησιμοποιεί δεδομένα για την ηλεκτρονική προώθηση διαφημιστικών μηνυμάτων και ενημερώσεων,
- τα πολιτικά κόμματα,
- οι θρησκευτικές οργανώσεις και οργανισμοί,
- οι διαφημιστικές και εταιρίες και οι εταιρίες δημοσκοπήσεων,
- οι ΜΚΟ που δραστηριοποιούνται σε τομείς όπως οι πρόσφυγες ή οι κοινωνικές μειονότητες.



Σχήμα 1: Έρευνα της Intrum σχετικά με τη συμμόρφωση των επιχειρήσεων με τον GDPR

(Πηγή: Εφημερίδα «Η Καθημερινή» στις 23/5/2018)

Αρκετοί, πάντως, οργανισμοί του ιδιωτικού τομέα, και κυρίως οι θυγατρικές πολυεθνικών ομίλων, έχουν συμμορφωθεί προς τη νέα οδηγία, ενώ ήδη από τις τελευταίες ημέρες πριν την παρέλευση της προθεσμίας συμμόρφωσης με τον GDPR, οι Έλληνες καταναλωτές λάμβαναν και λαμβάνουν σχετικά μηνύματα από λιανεμπορικές αλυσίδες, προκειμένου να συναινέσουν στη χρήση των προσωπικών τους δεδομένων.

Ωστόσο, ο βαθμός συμμόρφωσης των ελληνικών επιχειρήσεων και κυρίως των μικρομεσαίων παραμένει χαμηλός. Σύμφωνα με πανευρωπαϊκή έρευνα της σουηδικής εισπρακτικής εταιρείας Intrum, όπως δημοσιεύτηκε στην εφημερίδα «Η ΚΑΘΗΜΕΡΙΝΗ» στις 23 Μαΐου 2018 και παρουσιάζεται στο παρακάτω (Σχήμα 1), το 69% των επιχειρήσεων στην Ελλάδα δεν ήταν έγκαιρα ενημερωμένες για τον νέο Κανονισμό. Πρόκειται για το υψηλότερο ποσοστό που καταγράφεται στην έρευνα, ενώ συνολικά στην Ευρώπη το ποσοστό των επιχειρήσεων που δεν έχουν ακούσει για τον GDPR ανέρχεται σε 27%. Ειδικά σε ό,τι αφορά τις μεγάλες επιχειρήσεις, με περισσότερους από 250 εργαζομένους, το αντίστοιχο ποσοστό πανευρωπαϊκά είναι 12% και θεωρείται υψηλό. Σημειώνεται ότι η έρευνα είχε διεξαχθεί από τις 24 Ιανουαρίου έως τις 23 Μαρτίου 2018.

Σύμφωνα με την ίδια έρευνα, το κόστος συμμόρφωσης με τον νέο κανονισμό υπολογίζεται ότι είναι περίπου 8.000 ευρώ για μια μικρομεσαία επιχείρηση και φτάνει τα 65.000 ευρώ για μια μεγάλη. Με βάση τα παραπάνω, το συνολικό κόστος συμμόρφωσης με τον GDPR για τις επιχειρήσεις στην Ευρώπη εκτιμάται σε 198 δισ. ευρώ.

Συνεπώς, η Ελλάδα βρίσκεται ακόμα αρκετά πίσω σε σχέση με τα υπόλοιπα κράτη-μέλη ως προς την ετοιμότητα και τη συμμόρφωση των ιδιωτικών επιχειρήσεων με τον Κανονισμό, θέτοντας το ερώτημα αν η αιτία γι' αυτό είναι η ανεπαρκής πληροφόρηση, το υψηλό κόστος προετοιμασίας, η οικονομική κρίση της χώρας ή ο συνδυασμός όλων των παραπάνω.

4.3. Ο DPO στο δημόσιο τομέα

Όσον αφορά το δημόσιο τομέα, υποχρέωση διορισμού DPO έχουν όλες οι δημόσιες αρχές και υπηρεσίες (εκτός από τα δικαστήρια, όταν ασκούν δικαιοδοτικό έργο) και μάλιστα στο επίπεδο όπου γίνεται η συλλογή και επεξεργασία των δεδομένων. Στο πλαίσιο του συντονισμού της ασφάλειας στον τομέα του Δημοσίου, όλοι οι φορείς καλούνται να ορίσουν Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων, ο οποίος θα λειτουργεί ως σύνδεσμος με τη Γενική Γραμματεία Ψηφιακής Πολιτικής και θα εκπροσωπεί το φορέα του.

Αυτό σημαίνει ότι DPO οφείλουν να ορίσουν, ενδεικτικά:

- όλα τα δημόσια σχολεία, οι σχολές Ανώτατης και Ανώτερης Εκπαίδευσης, οι Επαγγελματικές σχολές κλπ.,
- όλα τα Υπουργεία και ξεχωριστά οι Γενικές Γραμματείες αυτών, αλλά (υπό προϋποθέσεις) και οι Διευθύνσεις και τα Τμήματα αυτών, ανάλογα με την επεξεργασία που πραγματοποιούν,
- όλοι οι φορείς που παρέχουν υπηρεσίες κοινής ωφέλειας, ακόμα και αν είναι εταιρίες ιδιωτικού δικαίου, όπως οι πάροχοι υπηρεσιών ενέργειας, μεταφορών, υποδομών, ραδιοτηλεοπτικών υπηρεσιών, επαγγελματικοί σύλλογοι με χαρακτήρα ΝΠΔΔ για τα πειθαρχικά τους συμβούλια (ΔΕΗ, ΕΡΤ, Οργανισμοί Λιμένος, ΔΕΔΔΗΕ, ΟΑΣΑ, ΣΤΑΣΥ, Δικηγορικοί Σύλλογοι, ΤΕΕ κλπ.),
- όλο οι ΟΤΑ και οι Επιχειρήσεις αυτών,
- όλες οι ανεξάρτητες διοικητικές αρχές.

Ωστόσο, μέχρι σήμερα και σύμφωνα με στελέχη του δημοσίου τομέα, οι φορείς που έχουν ορίσει τον Υπεύθυνο Προστασίας Δεδομένων είναι ελάχιστοι, ενώ ουσιαστικές ενέργειες για την πρακτική εφαρμογή του GDPR στον Δημόσιο Τομέα δεν έχουν γίνει ευρέως γνωστές, με αποτέλεσμα η συμμόρφωση των κρατικών υπηρεσιών με τον Κανονισμό αυτό, να μένει ακόμα «πίσω» σε σχέση με τον ιδιωτικό τομέα.

Ακόμα και η Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ), η οποία είναι το μεγαλύτερο κέντρο επεξεργασίας δεδομένων του ελληνικού Δημοσίου και διατηρεί ένα από τα μεγαλύτερα μητρώα (φορολογουμένων), δεν έχει ορίσει DPO, ενώ το θέμα της εφαρμογής του GDPR θα την απασχολήσει μετά την 25η Μαΐου.

Εξίσου κρίσιμος τομέας είναι εκείνος της υγείας (νοσοκομεία, ιατρικά κέντρα κ.λπ.), όπου ελάχιστη δουλειά έχει γίνει και στο επίπεδο αυτό, ενώ φαίνεται ότι σε όλες τις τεχνικές συναντήσεις που πραγματοποιήθηκαν σε κοινοτικό επίπεδο (Βρυξέλλες κ.ά.), η ελληνική πλευρά απουσίαζε συνεχώς.

Επιπλέον, στελέχη της δημόσιας διοίκησης θεωρούν ακόμα ότι η μη εφαρμογή του GDPR δεν θα έχει επιπτώσεις στο ελληνικό Δημόσιο. Κι αυτό διότι, όπως υποστηρίζουν, ακόμη και αν η ΑΠΔΠΧ επιβάλλει πρόστιμα σε δημόσιους φορείς, το ποσό απλώς θα μεταφερθεί από έναν κωδικό του κρατικού προϋπολογισμού σε έναν άλλο κωδικό, αρά δεν συντρέχει ιδιαίτερος λόγος επίσπευσης των διαδικασιών συμμόρφωσης. Τέλος, επισημαίνουν ότι, από το 1997 που υφίσταται η ΑΠΔΠΧ, το μοναδικό πρόστιμο σε δημόσιο φορέα που επιβλήθηκε για πλημμελή χρήση των προσωπικών δεδομένων ήταν το 2013 στη ΓΓΠΣ, 150.000 ευρώ, το οποίο είναι άγνωστο, αν έχει εισπραχθεί.

Η κατάσταση, όμως, δεν είναι έτσι και χρήζει άμεσης αντιμετώπισης, καθώς ο νέος Κανονισμός καθιστά πιο εύκολες τις προσφυγές αποζημίωσης των ιδιωτών για κακή χρήση των προσωπικών δεδομένων. Τη δυνατότητα αυτή προέβλεπε και ο νόμος 2472/1997, αλλά σε μικρότερη κλίμακα, γι' αυτό και τώρα όλοι εκτιμούν ότι οι προσφυγές θα γίνουν πιο εύκολες, με τους προσφεύγοντες να αξιώνουν μεγάλα ποσά, ενώ αναμένεται οι σχετικές νομικές διαδικασίες να διαρκούν μεγάλο χρονικό διάστημα.

Ενδεικτικό παράδειγμα για το δημόσιο τομέα αποτελεί το Υπουργείο Υγείας, το οποίο στο πλαίσιο της προσπάθειας για τη συντονισμένη οργάνωση και προετοιμασία του συνόλου των εποπτευόμενων φορέων καθώς επίσης και των ιδιωτικών φορέων παροχής υπηρεσιών υγείας, σχετικά με την ανάγκη συμμόρφωσης σε σχέση με τα οριζόμενα στον GDPR, προέβη, ως πρώτο βήμα, στον ορισμό Υπευθύνου Προστασίας Δεδομένων (DPO).

Ο Υπεύθυνος Προστασίας Δεδομένων του Υπουργείου Υγείας έχει ως έργο τη συνδρομή και το συντονισμό των Υπευθύνων Προστασίας Δεδομένων, τους οποίος θα ορίσουν οι εποπτευόμενοι φορείς, όσον αφορά τις απαιτήσεις γενικής συμμόρφωσης προς τις διατάξεις του Κανονισμού.

Ως δεύτερο βήμα, το Υπουργείο Υγείας προέβη στη σύνταξη σχετικής εγκυκλίου για την ενίσχυση των δράσεων συμμόρφωσης ως προς το GDPR, με περιεχόμενο:

1. Τη συνοπτική παρουσίαση του GDPR και των θεμελιωδών αρχών του.
2. Τις βασικές απαιτήσεις προετοιμασίας και εφαρμογής από την πλευρά των φορέων και παρόχων υπηρεσιών υγείας (δημόσιων και ιδιωτικών).
3. Το πλαίσιο ανάθεσης καθηκόντων των DPOs και των αναπληρωτών τους, καθώς επίσης και την οργάνωση διαδικασίας εσωτερικής πρόσκλησης εκδήλωσης ενδιαφέροντος από στελέχη των ιδίων των φορέων ή της διαδικασίας ανοικτών δημόσιων διαγωνισμών για την πλήρωση των θέσεων.
4. Επιλογή από συνήθη ερωτήματα και προβληματισμούς, που έχουν ήδη τεθεί προς τον DPO του Υπουργείου Υγείας από το διοικητικό και ιατρονοσηλευτικό προσωπικό σε σχέση με τις υποχρεώσεις των φορέων και τα δικαιώματα των ασθενών.
5. Τη διαδικασία διενέργειας των απαιτούμενων Μελετών Αντικτύπου.

Στο πλαίσιο αυτό, η εγκύκλιος σαφώς δεν περιορίζεται μόνο στην περίπτωση των δημόσιων φορέων, αλλά δύναται να αποτελέσει και μια προσπάθεια παροχής βασικών οδηγιών σχετικά με τη συμμόρφωση και των ιδιωτών παρόχων υπηρεσιών υγείας, στη λογική της εθνικής προετοιμασίας του τομέα της υγείας και της ενδυνάμωσης της προστασίας των πολιτών έναντι της επεξεργασίας δεδομένων τους προσωπικού χαρακτήρα.

Ο σχεδιασμός και η υλοποίηση της στρατηγικής του Υπουργείο Υγείας πραγματοποιείται με γνώμονα την προστασία των δεδομένων (ευαίσθητων και μη) προσωπικού χαρακτήρα, την απλοποίηση των διαδικασιών και τη μείωση της γραφειοκρατικής ταλαιπωρίας των πολιτών, τη λειτουργική εκπαίδευση των επαγγελματιών υγείας και την συντονισμένη ενδυνάμωση των εμπλεκομένων φορέων και παρόχων υπηρεσιών υγείας, με σκοπό τη συνολικότερη αναβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών.

Έτσι λοιπόν, το Υπουργείο Υγείας, από τους ελάχιστους δημόσιους φορείς που έχουν αρχίσει να συμμορφώνονται με τον GDPR και να ορίζουν DPO, έχει δημιουργήσει διευθύνσεις ηλεκτρονικού ταχυδρομείου για την επικοινωνία με τον αρμόδιο Υπεύθυνο Προστασίας Δεδομένων, ενώ αναμένεται η σταδιακή δημιουργία ενότητας ενημερωτικού χαρακτήρα στο διαδικτυακό του τόπο, σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα στον τομέα της υγείας, καθώς η προστασία του ατόμου έναντι της επεξεργασίας δεδομένων του προσωπικού χαρακτήρα δεν συνιστά απλή επιλογή, αλλά πρωταρχικό σκοπό του συστήματος.

4.4. Η ευθύνη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Με το νέο Κανονισμό, κάθε εποπτική αρχή, αποκτά και διευρυμένες εξουσίες. Ειδικότερα, κάθε Αρχή διαθέτει την εξουσία να απευθύνει προειδοποιήσεις, επιπλήξεις, να εκδίδει εντολές αλλά και να επιβάλλει πολύ σοβαρά διοικητικά πρόστιμα σε περίπτωση μη συμμόρφωσης με τον GDPR, που μπορεί να ανέλθουν έως και 20.000.000€ ευρώ ή στο 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, όποιο από τα δύο είναι μεγαλύτερο.

Ουσιαστικά η ΑΠΔΠΧ είναι αρμόδια να ελέγχει τη συμμόρφωση των φορέων και να επιβάλλει πρόστιμα ανάλογα με τη σοβαρότητα της παραβίασης και από το εάν ο οργανισμός θεωρείται ότι

έλαβε σοβαρά υπόψιν του εφαρμοστέα μέτρα και κανόνες σχετικά με την ασφάλεια της προστασίας των δεδομένων.

Συνεπώς, οφείλει να ελέγχει τη συμμόρφωση των οργανισμών με βάση:

- Καταγγελίες από πελάτες – προμηθευτές – συνεργάτες – εργαζομένους σε έτερες δημόσιες αρχές.
- Δικαστικές διαδικασίες (για χρηματική ικανοποίηση λόγω ηθικής βλάβης ή για ποινική ευθύνη).
- Απώλεια πιστοποιήσεων που έχουν οι επιχειρήσεις σε σχέση με πρότυπα λειτουργίας τους.
- Μη έγκαιρη πρόσληψη ή μη ύπαρξη Υπευθύνου Προστασίας Δεδομένων, εφόσον οι φορείς υποχρεούνται να διορίζουν DPO.
- Υποχρέωση γνωστοποίησης των επιχειρήσεων στην ΑΠΔΠΧ τυχόν παραβιάσεων προσωπικών δεδομένων (data breaches), ειδικά όταν ενδέχεται να τεθούν σε κίνδυνο τα δικαιώματα και οι ελευθερίες των ατόμων και να οδηγηθούν σε διακρίσεις, οικονομικές απώλειες, απώλεια εμπιστευτικότητας ή οποιοδήποτε άλλο οικονομικό ή κοινωνικό μειονέκτημα.

4.5. Προβληματισμοί σχετικά με την ύπαρξη και διεξαγωγή ελέγχων συμμόρφωσης στην Ελλάδα

Παρ΄ ολο που σε άλλα κράτη-μέλη (π.χ. Κύπρος) έχει ήδη ανακοινωθεί, από τις αρμόδιες εποπτικές αρχές η διεξαγωγή ελέγχων σε οργανισμούς τόσο του δημόσιου όσο και του ιδιωτικού τομέα, με σκοπό να διαπιστωθεί η συμμόρφωση τους με τον GDPR, στην Ελλάδα δεν έχει γίνει ακόμα γνωστή καμία τέτοια πρωτοβουλία. Αυτό έχει ως αποτέλεσμα να εγείρονται ερωτήματα αναφορικά με το σχεδιασμό και την υλοποιήση τέτοιου είδους ελέγχων. Συγκεκριμένα, αναμένονται διευκρινήσεις σχετικά με:

1. Τα άτομα που θα διενεργούν τους ελέγχους. Θα ορίζει η ΑΠΔΠΧ εσωτερικούς συνεργάτες της ή θα εξουσιοδοτεί εξωτερικές εταιρείες εμπειρογνομώνων;
2. Τους τρόπους και τα μέσα που θα επιτυγχάνονται οι έλεγχοι συμμόρφωσης στην Ελλάδα.
3. Πόσο συχνά θα διενεργούνται οι έλεγχοι, θα απαιτούνται επιτόπιοι έλεγχοι σε συνεργασία με τους DPOs των επιχειρήσεων, ποιους τομείς ασφαλείας θα ελέγχουν, κτλ.;
4. Πώς θα εξασφαλίζεται η αμεροληψία και η εμπιστοσύνη των συνεργατών της ΑΠΔΠΧ;
5. Με ποιον τρόπο θα εξακριβώνεται η ικανότητα του DPO να διενεργεί ελέγχους, δεδομένης της μη ύπαρξης και μη υποχρέωσης επίσημης πιστοποίησης ούτε από τον GDPR ούτε από τις αρμόδιες εποπτικές αρχές;
6. Πώς θα εξασφαλίζεται η συμμόρφωση με τον GDPR και η ύπαρξη DPO (σε περιπτώσεις υποχρεωτικού διορισμού του); Θα θεσπιστεί κάποιου είδους πιστοποίηση ασφαλείας;
7. Πώς θα βεβαιώνονται τα πρόστιμα και οι κυρώσεις όταν δεν θα συμμορφώνονται οι διάφοροι οργανισμοί; Θα ακολουθούνται οι ίδιες διαδικασίες είτε για ιδιωτικούς είτε για δημόσιους φορείς;

Συνεπώς, γίνεται αντιληπτό ότι η ολιγωρία των αρμόδιων αρχών δημιουργεί ερωτήματα ως προς την εφαρμογή της θεωρίας στην πράξη και δυσχεραίνει ακόμα περισσότερο τη δημιουργία ενός ενιαίου πρωτοκόλλου ελέγχου συμμόρφωσης με τον GDPR.

5. Συμπεράσματα

Ο ρόλος του DPO αποδεικνύεται ότι είναι κρίσιμης σημασίας στην εναρμόνιση της εταιρείας με τον GDPR, αφού καθίσταται υπεύθυνος για τη συνεχή παρακολούθηση των εργασιών μετάβασης στα νέα δεδομένα αλλά και αρμόδιος για τον έλεγχο τόσο των ενεργειών του υπευθύνου και του εκτελούντος την επεξεργασία των δεδομένων, όσο και για τη συμβουλευτική υποστήριξη και εκπαίδευση του προσωπικού. Οφείλει να έχει όλα τα απαραίτητα προσόντα που θα τον κάνουν αποτελεσματικότερο στην εκπλήρωση των στόχων του οργανισμού και τα οποία θα μπορούν να

δικαιολογούν και την ανάλογη αμοιβή του. Ωστόσο, βρίσκεται στη διάθεση της επιχείρησης η επιλογή του αν ο DPO θα είναι εσωτερικός ή εξωτερικός συνεργάτης, αφού πρέπει να λαμβάνεται υπόψιν τόσο η αμεροληψία και οι ικανότητές του, όσο και το κόστος του για την επιχείρηση σε κάθε περίπτωση.

Με γνώμονα τα παραπάνω, τέθηκαν οι προβληματισμοί σχετικά με την ετοιμότητα των επιχειρήσεων και ιδίως του δημοσίου τομέα στα πλαίσια συμμόρφωσης με τον GDPR, όπου διαπιστώνεται η ανεπάρκεια σχεδίου δράσης και οργάνωσης για τον έλεγχο τόσο εσωτερικών τους διαδικασιών όσο και επιβολής κυρώσεων σε τρίτους φορείς. Σχετικά με τον ορισμό του Υπεύθυνου Προστασίας Δεδομένων και γενικότερα, τη συμμόρφωση με τις απαιτήσεις του Κανονισμού, τίθενται κρίσιμα διλήμματα για κάθε φορέα, είτε είναι επιχείρηση είτε είναι οργανισμός ως προς το αν αποτελεί άλλη μια τυπική, κανονιστική, κοστοβόρα και γραφειοκρατική διαδικαστική υποχρέωση ή πρόκληση για τον εκσυγχρονισμό κάθε φορέα και ευκαιρία να ενισχυθεί στην πράξη ο σεβασμός στην προσωπικότητα κάθε ατόμου.

Συμπεραίνεται λοιπόν, ότι η συμμόρφωση με τον GDPR είναι μια διαρκής διαδικασία., που απαιτεί να γίνει εξ' αρχής ορθή υλοποίηση. Σ' αυτό θα συμβάλλει αποτελεσματικά η κρίση και οι ενέργειες του DPO, ώστε να καλλιεργηθεί συστηματικά, σε κάθε τμήμα και υπάλληλο του οργανισμού, η πολύτιμη κουλτούρα του σεβασμού της προστασίας δεδομένων. Διότι σκοπός δεν είναι η εφαρμογή του Κανονισμού «στα χαρτιά» αλλά η πρακτική εφαρμογή του, ώστε αλλάζοντας την κουλτούρα των επιχειρήσεων και των οργανισμών, να επιτευχθεί η βελτίωση των επιχειρηματικών διαδικασιών καθώς και η διαφύλαξη των προσωπικών δεδομένων που διαχειρίζονται.

Βιβλιογραφία

Kathimerini.com.cy (2018). *Δεν προλαβαίνουν όλοι για τα προσωπικά δεδομένα*., Ηρακλέους Μ., Ανακτήθηκε από http://www.kathimerini.com.cy/gr/oikonomiki/epixeiriseis/den-prolabainoyn-oloi-gia-ta-prosopika-dedomena στις 15 Ιουλίου 2018.

Kathimerini.gr (2018). *Ανέτοιμοι για τον κανονισμό προστασίας προσωπικών δεδομένων, του Μανδραβέλης Β., Μανιφάβα Δ. Α*νακτήθηκε από: http://www.kathimerini.gr/965735/gallery/oikonomia/ellhnikh-oikonomia/anetoimoi-gia-ton-kanonismo-prostasias-proswpikwn-dedomenwn στις 3 Αυγούστου 2018.

Kathimerini.gr (2018). *Άποψη - GDPR: ένα στενό κοστούμι ή ορθή επιχειρηματική πρακτική;, Αναστασάκης Λ. Α*νακτήθηκε από http://www.kathimerini.gr/978353/article/oikonomia/ellhnikh-oikonomia/apoyh---gdpr-ena-steno-kostoymi-h-or8h-epixeirhmatikh-praktikh στις 22 Σεπτεμβρίου 2018.

Ustaran, E., & Lovells, H. (2018). *European Data Protection, Law and Practice*. Portsmouth, NH: International Association of Privacy Professionals (IAPP) Publication.

Voigt, P. & von dem Bussche, A. (2017). *The Eu General Data Protection Regulation*. New York: Springer International Publishing.

Δημουλά, Ε. (2018). *Εφαρμογή του Νέου Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (EU 2016/679) στην ελληνική πραγματικότητα.* Μεταπτυχιακή Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών: «Τεχνο –οικονομικά συστήματα», ΕΜΠ-Πανεπιστήμιο Πειραιώς

Ιγγλεζάκης, Ι. (2018). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679)*. Θεσσαλονίκη: Εκδόσεις Interactive.

Καμπούρης, Α. (2015). *Εκτίμηση των Επιπτώσεων Σχετικά με την Προστασία των Δεδομένων*, Μεταπτυχιακή Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών: «Τεχνο –οικονομικά συστήματα», ΕΜΠ-Πανεπιστήμιο Πειραιώς.

Κανονισμός *2016/679/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (Γενικός Κανονισμός για την Προστασία Δεδομένων)*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 119/1 της 4/5/2016. Ανακτήθηκε από http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679 στις 20 Ιουλίου 2018.

Κοτσαλής, Λ., & Μενουδάκος, Κ. (2018). *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή*. Νομική Βιβλιοθήκη ΑΕΒΕ.

Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων, *Guidelines on Data Protection Officers ('DPOs')*. Ανακτήθηκε από http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 στις 2 Αυγούστου 2018.

Πλατής, Ε. (2018). *Μικρές Συλλογές*: *Προσωπικά Δεδομένα-Προστασία GDPR*. 1η έκδοση. Αθήνα: Εκδόσεις Παπαδόπουλος.

Σιασιάκος, Κ., Αναστασίου, Σ., & Τούντας, Κ. (2016). *Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης*. http://dx.doi.org/10.12681/elrie.817

Σωτηρόπουλος, Β. (2017). *Υπεύθυνος Προστασίας Δεδομένων, Εργαλειοθήκη για το νέο θεσμό σε δημόσιο και ιδιωτικό τομέα*. Εκδόσεις Σάκκουλα.