ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ

Διπλωματική Εργασία

ΕΦΑΡΜΟΓΗ ΚΑΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR) ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ (ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΕΩΝ)

Της

ΚΑΤΣΑΒΡΙΑ ΔΗΜΗΤΡΑΣ ΤΟΥ ΘΩΜΑ

Επιβλέπων Καθηγητής: κ. **ΛΙΒΑΝΗΣ ΕΥΣΤΡΑΤΙΟΣ**

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη

Λογιστική και Χρηματοοικονομική

Οκτώβριος, 2018

ΕΥΧΑΡΙΣΤΙΕΣ

Η εκπόνηση της παρούσης διπλωματικής εργασίας, πραγματοποιήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών στη Λογιστική και Χρηματοοικονομική, του τμήματος Λογιστικής Και Χρηματοοικονομικής του Πανεπιστημίου Μακεδονίας.

Σε μια συνεχή προσπάθεια για δια βίου μόρφωση και επιμόρφωση, το προκείμενο εκπαιδευτικό αντικείμενο, έρχεται να προστεθεί στα παρελθόντα εκπαιδευτικά επιτεύγματα, με σκοπό να οδηγήσουν σε διδακτορική έρευνα και στην εξαγωγή χρήσιμων αποτελεσμάτων.

Πρωτίστως αμέριστη ευγνωμοσύνη και θερμές ευχαριστίες για τα τόσα, και για τα άλλα τόσα χρόνια αέναης και ανιδιοτελής στήριξης και ενθάρρυνσης, θα ήθελα να εκφράσω στους γονείς μου Θωμά και Ανδρομάχη, καθώς και στον αδελφό μου Κωνσταντίνο που σπουδάζει στη Σάμο. Η παρούσα διπλωματική εργασία αφιερώνεται σε εσάς ως ένδειξη ευγνωμοσύνης για τα όσα έχετε προσφέρει σε εμένα.

Στη συνέχεια θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Λιβάνη Ευστράτιο, (παρά τις συγκυρίες που προέκυψαν), για την συμβολή του στην επιλογή της θεματολογίας, καθώς και για την καθοδήγησή του. Επιπλέον θα ήθελα να ευχαριστήσω όλους τους καθηγητές του προγράμματος, για τις γνώσεις που μου παρήχαν, εφόδια για την μετέπειτα επαγγελματική μου πορεία.

Τέλος δεν θα μπορούσα να μην ευχαριστήσω τον κ. Ευαγγελίδη Αντώνη Διευθυντή Εταιρικής Συμμόρφωσης & Προστασίας Δεδομένων (DPO), για το χρόνο που διέθεσε στο να με βοηθήσει να κατανοήσω καλύτερα τον νέο αυτό Κανονισμό, καθώς και στο πλούσιο υλικό που μου παρήχε. Χωρίς την συμβολή του δεν θα μπορούσε να υλοποιηθεί η παρούσα διπλωματική εργασία. Ακόμη ευχαριστώ πολύ και την Κανονιστική Διεύθυνση της Τράπεζας που μελετάτε παρακάτω για το υλικό που μου παρείχε.

ΠΕΡΙΛΗΨΗ

Η ραγδαία εξέλιξη της τεχνολογίας και των μέσων επικοινωνίας είναι ένα φαινόμενο που έχει επηρεάσει μια πληθώρα τομέων της σύγχρονης ζωής του ανθρώπου. Καθώς η ταχέως μεταβαλλόμενη τεχνολογία καθιστά όλο και πιο διαθέσιμες τις πληροφορίες, οι μελετητές, και οι υπεύθυνοι για τη χάραξη πολιτικής προσπαθούν να καθορίσουν την ιδιωτικότητα, ενώ πολλοί παραδέχονται ότι το καθήκον αυτό είναι σχεδόν αδύνατο.

Στην κατανόηση της ιδιωτικής ζωής υπάρχει μια αντικειμενική δυσκολία για την οριοθέτηση των αλληλοσυμπληρούμενων εννοιών. Κανένας ορισμός δεν μπορεί να λειτουργήσει, επειδή μάλλον υπάρχουν πολλαπλές μορφές ιδιωτικού απορρήτου, που σχετίζονται μεταξύ τους με οικογενειακές ομοιότητες. Μια θεωρία του γεφυρώνει πολιτισμικές διαφορές και αντιμετωπίζει τις ιστορικές αλλαγές στις απόψεις για την ιδιωτικότητα είναι καίριας σημασίας για την προστασία των δεδομένων προσωπικού χαρακτήρα από ηλεκτρονικές επικοινωνίες Η προστασία των δεδομένων προσωπικού χαρακτήρα είναι αυξημένης σημασίας δεδομένου ότι πρόκειται για ένα θεμελιώδες δικαίωμα του ανθρώπου.

Στην Ελλάδα η σχετική νομοθεσία έχει εναρμονιστεί με το Ευρωπαϊκό νομοθετικό πλαίσιο και συνεχίζει να υιοθετεί κανόνες και ρυθμιστικές διατάξεις που να προστατεύουν τις συγκεκριμένες σημαντικές προεκτάσεις των ηλεκτρονικών επικοινωνιών και της προστασίας των προσωπικών δεδομένων, όπως είναι η είσοδος στις ζωές μας δια νόμου του GDPR.

Στην παρούσα εργασία θα παρουσιαστούν οι νομικές ιστορικές πτυχές της προστασίας των προσωπικών δεδομένων, καθώς και τα βήματα προετοιμασίας που πρέπει να ακολουθήσει μια επιχείρηση για την μετάβασή της στον GDPR καθώς και τον ρόλο που διαδραματίζει ο DPO. Στο πλαίσιο αυτό, θα παρουσιαστεί το στρατηγικό σχέδιο και οι φάσεις υλοποίησης συμμόρφωσης με τον GDPR μιας ελληνικής φαρμακευτικής εταιρείας, καθώς και μιας εγχώριας συστημικής Τράπεζας, με στόχο τη σύγκριση του θεωρητικού υποβάθρου του νέου Κανονισμού, με την πρακτική του εφαρμογή.

Λέξεις κλειδιά: Προσωπικά Δεδομένα, Υποκείμενο των Δεδομένων, Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR), Αρχή Προστασίας

Δεδομένων Προσωπικού Χαρακτήρα, Υπεύθυνος Προστασίας Δεδομένων, Υποχρέωση Γνωστοποίησης Παραβιάσεων, Εκτίμηση Αντικτύπου, Μεθοδολογία Συμμόρφωσης, Υλοποίηση Στρατηγικού Πλάνου.

ABSTRACT

The rapid development of technology and the media is a phenomenon that has affected many areas of modern human life. As rapidly changing technology makes information more and more available, scholars and policymakers are trying to determine privacy, and many admit that this task is almost impossible.

In understanding the privacy there is an objective difficulty in defining complementary concepts. No definition can work, because there are multiple forms of privacy that are related to family similarities. A theory of bridging cultural differences and facing historical changes in views on privacy is crucial to the protection of personal data by electronic communications The protection of personal data is of increasing importance as it is a fundamental human right.

In Greece, the relevant legislation has been aligned with the European legislative framework and continues to adopt rules and regulations to protect the specific significant extensions of electronic communications and personal data protection, such as the entry into our lives by GDPR law.

This postgraduate thesis will present the legal historical aspects of personal data protection as well as the steps that a company must take to move to the GDPR and the role of the DPO. In this context, the strategic plan and the phases of compliance with GDPR of the Greek pharmaceutical company VIANEX and the Bank will be presented, aiming to compare the theoretical background of the new Regulation with its practical application.

Key Words: Personal Data, Data Subject, General Data Protection Regulation (GDPR), Hellenic Data Protection Authority, Data Protection Officer (DPO), Data Breaches Notification, Data Protection Impact Assessment, Compliance Methodology, Strategic Plan Implementation.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ

1.1 Σκοπός και Αντικείμενος της εργασίας 6

1.2 Διάρθρωση κεφαλαίων της διπλωματικής 7

ΚΕΦΑΛΑΙΟ 2 ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 Εισαγωγή 9

2.2 Σύντομη ιστορική αναδρομή στα προσωπικά δεδομένα 9

2.3 Η Ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών Δεδομένων 11

2.4 Η Ελληνική νομοθεσία περί προστασίας προσωπικών δεδομένων 17

2.5 Η ελληνική εποπτική «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα» 20

2.6 Σύνοψη 25

ΚΕΦΑΛΑΙΟ 3 : Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩ ΔΕΔΟΜΕΝΩΝ (GDPR)

3.1 Εισαγωγή 26

3.2 Ανάλυση περιεχομένου του GDPR 27

3.3 Η έννοια της συγκατάθεσης 33

3.4 Εκτίμηση αντίκτυπου σχετικά με την προστασία προσωπικών δεδομένων (DPIA) 35

3.4.1 Επιπτώσεις από την εφαρμογή του GDPR στις ελληνικές επιχειρήσεις 37

3.4.2 Επιπτώσεις από την επιβολή του GDPR στον Δημόσιο Τομέα 39

3.5 Πρόστιμα και κυρώσεις 40

3.6 Πρόσθετες επιπτώσεις για τα φυσικά πρόσωπα από τον GDPR 43

3.6.1 Το GDPR για τα παιδιά 46

3.7 Πρόσθετες επιπτώσεις για τις επιχειρήσεις από την επιβολή του GDPR (άμεσα-έμμεσα κόστη) 48

3.8 Σύνοψη 53

ΚΕΦΑΛΑΙΟ 4 : ΥΠΟΧΡΕΩΤΙΚΟΣ ΟΡΙΣΜΟΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)

4.1 Εισαγωγή 54

4.2 Υποχρεωτικός Ορισμός DPO 55

4.3 Προσόντα διορισμού ενός DPO 59

4.4 Καθήκοντα ενός DPO 64

4.5 Σύνοψη 66

ΚΕΦΑΛΑΙΟ 5 : ΜΕΘΟΔΟΛΟΓΙΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

5.1 Εισαγωγή 67

5.2 Βήματα συμμόρφωσης με τον GDPR 69

5.3 Μεθοδολογία Συμμόρφωσης με τον GDPR 75

5.4 Εκπαίδευση του ανθρώπινου δυναμικού 82

5.5 Διαμόρφωση ηθικής νοοτροπίας και επικαιροποίηση του GDPR 86

5.6 Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στην Ελλάδα 88

5.6.1 Η έρευνα της ICAP 88

5.6.2 Η έρευνα του ΣΕΒ 90

5.6 Σύνοψη 92

ΚΕΦΑΛΑΙΟ 6 : ΛΟΓΙΣΜΙΚΑ ΥΠΟΣΤΗΡΙΞΗΣ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗΣ ΤΟΥ ΝΕΟΥ ΚΑΝΟΝΣΜΟΥ ΑΠΟ ΜΕΓΑΛΕΣ ΕΤΑΙΡΕΙΕΣ ΛΟΓΙΣΜΙΚΩΝ

6.1 Εισαγωγή 93

6.2 Λογισμικά της εταιρείας ORACLE 95

6.3 Λογισμικά της εταιρείας Microsoft 102

6.4 Οι εταιρείες ως σύμβουλος συμμόρφωσης για το GDPR 109

6.4.1 Σύμπραξη των εταιρειών «Alcosystems» και «Priority» 109

6.4.2 SYNTAX Πληροφορική Α.Β.Ε.Ε. 110

6.4.3 Intracom Telecom 112

6.5 Σύνοψη 114

ΜΕΡΟΣ Β΄: ΜΕΛΕΤΗ ΠΕΡΙΠΩΣΕΩΝ

ΚΕΦΑΛΑΙΟ 7 : ΕΦΑΡΜΟΓΗ ΜΕΘΟΔΟΛΟΓΙΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΣΕ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΚΑΙ ΣΕ ΕΛΛΗΝΙΚΗ ΤΡΑΠΕΖΑ

7.1 Εισαγωγή 115

7.2. Εφαρμογή του GDPR σε μια ελληνική φαρμακευτική εταιρεία 115

7.2.1 Οδικός χάρτης προετοιμασίας του GDPR από μια ελληνική φαρμακευτική εταιρεία» 117

7.2.2 Φάσεις έργου συμμόρφωσης με τον GDPR 118

7.3 Εφαρμογή του GDPR από Ελληνική Τράπεζα 135

7.3.1 Φάσεις συμμόρφωσης με τον GDPR 137

7.3.2 GDPR και PSD II 142

7.4 Σύνοψη 144

ΚΕΦΑΛΑΙΟ 8 : ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

8.1 Συμπεράσματα 145

8.2 Περιορισμοί στην έρευνα 149

8.3 Προτάσεις για περαιτέρω έρευνα 149

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Εικόνα 1: Τα ευαίσθητα προσωπικά δεδομένα όπως αναφέρονται στην ευρωπαϊκή και στην ελληνική νομοθεσία 20

Εικόνα 2: Σημεία συμμόρφωσης στον Κανονισμό που δυσκολεύουν τις επιχειρήσεις, 2017-2018 39

Εικόνα 3: Ενέργειες προς αποφυγή για την μη επιβολή προστίμων 42

Εικόνα 4: Άμεσα και έμμεσα κόστη από την επιβολή του GDPR στις

Επιχειρήσεις 52

Εικόνα 5: Ποσοστιαίο κατά κεφαλήν άμεσο και έμμεσο κόστος της παραβίασης των δεδομένων 53

Εικόνα 6: Επισκόπηση των βασικών απαιτήσεων GDPR 75

Εικόνα 7 : Οδικός Χάρτης Συμμόρφωσης με τον GDPR 82

Εικόνα 8 : Όλες οι δράσεις που πρέπει να γίνουν για επιτυχή συμμόρφωση με τον GDPR 88

Εικόνα 9: Έρευνα για το επίπεδο συμμόρφωσης των επιχειρήσεων με τον Κανονισμό στην Ελλάδα 89

Εικόνα 10: Έρευνα για το επίπεδο συμμόρφωσης με τον GDPR των ελληνικών επιχειρήσεων-απαντήσεις και σε άλλες ερωτήσεις συναφείς με την συμμόρφωση 90

Εικόνα 11: Επιχειρήσεις σε Ελλάδα και Ευρώπη που δηλώνουν άγνοια για τον GDPR 93

Εικόνα 12: Βήματα συμμόρφωσης με τον GDPR που προτείνει η MICROSOFT 103

Εικόνα 13: Οδικός Χάρτης Ετοιμότητας της ελληνικής φαρμακευτικής εταιρείας με τον GDPR 118

Εικόνα 14: Φάσεις έργου συμμόρφωσης με τον GDPR 120

Εικόνα 15: Δημιουργία Ομάδας Έργου GDPR από την ελληνική φαρμακευτική εταιρεία 122

Εικόνα 16: Χρονοδιάγραμμα 1ης φάσης GDPR στην ελληνική φαρμακευτική εταιρεία 123

Εικόνα 17: GDRR Maturity Profile - Αξιολόγηση Βαθμού ετοιμότητας της ελληνικής φαρμακευτικής εταιρείας 125

Εικόνα 18: Απαιτούμενες Πολιτικές και Διαδικασίες 127

Εικόνα 19: Χρονοδιάγραμμα Εξέλιξης 2ης Φάσης GDPR στην ελληνική φαρμακευτική εταιρεία 129

Εικόνα 20: Τα 25 βήματα του Οδικού Χάρτη Υλοποίησης του GDPR στην ελληνική φαρμακευτική εταιρεία 131

Εικόνα 21: Χρονοδιάγραμμα Υλοποίησης GDPR στην ελληνική φαρμακευτική εταιρεία 134

ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ

1.1 Σκοπός και Αντικείμενο της Εργασίας

Είναι γεγονός ότι ο 21ος αιώνας χαρακτηρίζεται από αλματώδη βήματα στην τεχνολογία, στα μέσα ανταλλαγής των πληροφοριών δημιουργώντας μια νέα τάξη πραγμάτων στους χρήστες και στους συνδρομητές υπηρεσιών ηλεκτρονικών επικοινωνιών. Τα δεδομένα που ανταλλάσσονται καθημερινά μέσα από τις ηλεκτρονικές επικοινωνίες είναι παραπάνω από δισεκατομμύρια ενώ η επεξεργασία τους, είναι μια διαδικασία που παρουσιάζει ιδιαίτερο ενδιαφέρον από τη στιγμή που μπορεί το περιεχόμενο των πληροφοριών να αποτελέσει σημαντική γνώση για πολλούς φορείς που κυρίως προσπαθούν να αποτρέψουν εγκλήματα ή γενικά παράνομες ενέργειες.

Σε αυτή την αλματώδη ανάπτυξη, είναι φυσικό πως η προστασία των προσωπικών δεδομένων, συνδέεται άρρηκτα με το ίδιο το απόρρητο της πληροφορίας. Η ανάγκη αυτή της προστασίας των προσωπικών δεδομένων, κατέστησε αναγκαία τη θέσπιση ενός νέου ρυθμιστικού πλαισίου για την προστασία των προσωπικών δεδομένων, το οποίο να διευρύνει και να εξελίσσει τις ήδη υπάρχουσες μεθόδους προστασίας, αλλά και να διασφαλίζει ακόμη περισσότερο τα δικαιώματα των ανθρώπων.

Μέσα από την παρούσα διπλωματική εργασία, θα γίνει μια προσπάθεια να περιγραφούν και να κατανοηθούν οι νέες κατευθυντήριες γραμμές και αλλαγές που επιφέρει η εφαρμογή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR), που εφαρμόζεται στη χώρα μας από τις 25 Μαΐου 2018. Ακόμη θα μελετηθούν δύο ελληνικές οικονομικές οντότητες, που δραστηριοποιούνται σε κλάδους που επηρεάζονται άρδην από την εφαρμογή του νέου Κανονισμού. Ειδικότερα θα μελετήσουμε μια μεγάλη ελληνική φαρμακευτική τράπεζα, καθώς και μια ελληνική τράπεζα, σχετικά με τον στρατηγικό σχεδιασμό που υλοποίησαν και τις διαδικασίες-φάσεις που ακολούθησαν, ώστε να συμμορφωθούν με τον GDPR.

Επιπλέον θα παρουσιαστούν αναλυτικά κάποια νέα λογισμικά ή εφαρμογές που έχουν δημιουργηθεί από μεγάλες εταιρίες που ειδικεύονται σε πληροφοριακά προγράμματα, και τα οποία βρίσκονται στη διάθεση των υπευθύνων για την ομαλή συμμόρφωσή τους με τον GDPR. Τέλος ειδική αναφορά θα γίνει στο σημαντικό ρόλο

που διαδραματίζει ο υπεύθυνος προστασίας προσωπικών δεδομένων (DPO), ως συνδετικός κρίκος ανάμεσα στο GDPR και στην οικονομική οντότητα, καθώς και στις αρμοδιότητες με τις οποίες είναι επιβαρυμένος.

1.2 Διάρθρωση κεφαλαίων της διπλωματικής

Η διπλωματική εργασία, χωρίζεται σε δύο μέρη. Το πρώτο μέρος περιλαμβάνει αναλυτική βιβλιογραφική επισκόπηση σχετικά με τα όσα ορίζονται στον νέο Κανονισμό, τον GDPR και το δεύτερο μέρος απαρτίζεται από την μελέτη δύο περιπτώσεων.

Αναλυτικότερα, στο πρώτο μέρος της εργασίας, και συγκεκριμένα στο δεύτερο κεφάλαιο πραγματοποιείται μια σύντομη ιστορική αναδρομή σχετικά με τους νόμους και τους κανονισμούς που έχουν θεσπιστεί τόσο στην χώρα μας, όσο και στην Ευρώπη γενικότερα, όσον αφορά την προστασία των προσωπικών δεδομένων.

Το τρίτο κεφάλαιο, περιλαμβάνει αναλυτικά το νέο νομοθετικό πλαίσιο που ορίζει η επιβολή του νέου Κανονισμού 2016/680 (GDPR), που ισχύει επίσημα στην χώρα μας από τις 25 Μαΐου του 2018. Αναλύονται όλα τα νέα δεδομένα, οι ορισμοί και οι υποχρεώσεις που φέρνει ο νέος Κανονισμός, τόσο στην καθημερινότητα και τις ζωές των απλών πολιτών, όσο και στις οικονομικές οντότητες του τόπου, δημόσιες ή ιδιωτικές. Αναλύεται η πολύ σημαντική έννοια της «συγκατάθεσης, καθώς και η εισαγωγή ενός νέου όρου, της «διαδικασίας εκτίμησης αντικτύπου» σχετικά με την παραβίαση των προσωπικών δεδομένων, », που διαδραματίζουν σημαντικό ρόλο στην επιβολή του νέου Κανονισμού. Ακόμη, γίνεται αναφορά για τις περιπτώσεις από την επιβολή του νέου Κανονισμού στα φυσικά πρόσωπα, με ειδική αναφορά στην ευαίσθητη ομάδα των παιδιών. Τέλος αναλύονται οι οικονομικές συνέπειες για τους οργανισμούς δημόσιους ή ιδιωτικούς, με την επιβολή πολύ υψηλών προστίμων και κυρώσεων, καθώς και σε άλλα κόστη έμμεσα ή άμεσα που προκύπτουν από την υποχρεωτική επιβολή του νέου Κανονισμού.

Στο τέταρτο κεφάλαιο, περιγράφεται ο πολύ σημαντικός ρόλος του «Υπευθύνου Προσωπικών Δεδομένων», καθώς και ο υποχρεωτικός ορισμός από τις οικονομικές οντότητες, που επηρεάζονται από τον Κανονισμό. Πραγματοποιείται εκτενής

αναφορά, στα προσόντα που θα πρέπει να έχει για να διοριστεί κάποιος ως DPO, καθώς και στα καθήκοντα και τις προκλήσεις που θα πρέπει να αντιμετωπίσει.

Στο πέμπτο κεφάλαιο, αναπτύσσεται σε θεωρητικό επίπεδο τα βήματα προετοιμασίας και οι μεθοδολογίες που μπορούν να ακολουθήσουν οι οικονομικές οντότητες δημόσιες ή ιδιωτικές, προκειμένου να εντάξουν τον GDPR όσο πιο ανώδυνα γίνεται στην οργάνωση και στη λειτουργία του οργανισμού τους.

Στο έκτο και τελευταίο κεφάλαιο, του πρώτου μέρους της εργασίας, περιγράφονται οι κινήσεις που έκαναν οι μεγαλύτερες λογισμικές εταιρίες, σχετικά με την δημιουργία νέων εφαρμογών, ή την αναβάθμιση υπαρχόντων για να διευκολύνουν τις οικονομικές οντότητες στην ομαλή μετάβαση και συμμόρφωση με τις διατάξεις και τους κανόνες του GDPR. Ειδικότερα αναφέρονται λογισμικά από τις πιο γνωστές εταιρίες που δραστηριοποιούνται στη χώρα μας, όπως είναι η ORACLE και η MICROSOFT, καθώς και εταιρίες που ανέλαβαν τον ρόλο του συμβούλου όπως είναι η ALCOSYSTEMS σε σύμπραξη με την εταιρία PRIORITY, η SYNTAX ΠΛΗΡΟΦΟΡΙΚΗ Α.Β.Ε.Ε καθώς και η INTRACOM TELECOM.

Στο δεύτερο μέρος της παρούσης διπλωματικής εργασίας, γίνεται μια προσπάθεια σύνδεσης και αξιοποίησης όλων των προηγούμενων στοιχείων σχετικά με το θεωρητικό υπόβαθρο του νέου Κανονισμού, εφαρμοσμένα στην ελληνική πραγματικότητα. Ειδικότερα, μελετάτε η πρακτική εφαρμογή της μεθοδολογίας συμμόρφωσης με τον GDPR, από μία μεγάλη ελληνική φαρμακευτική εταιρία, όσο και από μία εγχώρια συστημική ελληνική Τράπεζα, δύο κλάδοι που επηρεάζονται άμεσα από τις διατάξεις του νέου Κανονισμού. Τα στοιχεία που παρουσιάζονται, έχουν προέλθει μετά από επικοινωνία που είχα προσωπικά με τους υπευθύνους προστασίας προσωπικών δεδομένων για την χορήγηση επιπλέων στοιχείων, καθώς και μετά από έρευνα που πραγματοποίησα στο διαδίκτυο.

Τέλος, στο όγδοο κεφάλαιο, παρουσιάζονται τα συμπεράσματα που εξήχθησαν από την ανάλυση και το σχεδιασμό του θέματος, καθώς και το αν έχουν απαντηθεί όλα τα θέματα που τέθηκαν σαν στόχοι. Επιπλέον προτείνονται θέματα για περαιτέρω έρευνα πάνω στο νέο Κανονισμό του GDPR.

ΜΕΡΟΣ Α: ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ

ΚΕΦΑΛΑΙΟ 2 : ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 Εισαγωγή

Η έννοια της «προστασίας των προσωπικών δεδομένων», δηλαδή πληροφοριών που προσδίδουν μια ιδιότητα, κάποια χαρακτηριστικά γνωρίσματα σε κάποιο άτομο, συναντάται από πολύ πριν εισβάλλει στη ζωή των ανθρώπων, η ηλεκτρονική τεχνολογία και ειδικότερα το διαδίκτυο Internet. Ωστόσο η αλματώδης ανάπτυξη των τεχνολογικών μέσων κατέστησε πιο επιτακτική την ενασχόληση με την έννοια των προσωπικών δεδομένων και με την προστασία αυτών.

Στο παρόν κεφάλαιο, θα παρουσιαστεί μια σύντομη ιστορική αναδρομή σχετικά με νόμους και κανονισμούς που θεσπίστηκαν από το 1950 έως και το 1990 σχετικά με την προστασία των προσωπικών δεδομένων. Στη συνέχεια θα παρουσιαστούν τα νομοθετήματα τόσο σε ευρωπαϊκό επίπεδο, όσο και σε εθνικό, με ιδιαίτερη έμφαση στο περιεχόμενο του Ν. 2472/1997 που ίσχυε μέχρι πρόσφατα στη χώρα μας, όπου εισήγαγε για πρώτη φορά δικαιώματα στα άτομα για κατοχύρωση και προστασία των προσωπικών τους δεδομένων. Ακόμη αποσαφηνίζονται οι πολύ σημαντικοί όροι των «προσωπικών δεδομένων», της «επεξεργασίας των δεδομένων», καθώς και κάποιων πολύ σημαντικών αρχών που εισήγαγε η Οδηγία 95/46/ΕΚ και θα πρέπει να τηρούνται κατά την επεξεργασία των προσωπικών δεδομένων. Τέλος αναλύονται τα καθήκοντα και οι αρμοδιότητες που οφείλουν να έχουν οι εποπτικές αρχές του κάθε τόπου, με εστίαση στην Ελληνική εποπτική Αρχή Προστασίας Προσωπικών Δεδομένων.

2.2 Σύντομη ιστορική αναδρομή στα προσωπικά δεδομένα

Στη Ρώμη, στις 4 Νοεμβρίου 1950, τα μέλη του Συμβουλίου της Ευρώπης, λαμβάνοντας υπόψη την «Παγκόσμια Δήλωση των Δικαιωμάτων του Ανθρώπου» που διακήρυξε η Γενική Συνέλευση των Ηνωμένων Εθνών (1948), υπέγραψαν την «Ευρωπαϊκή Σύμβαση για την προάσπιση των Ανθρωπίνων Δικαιωμάτων και των Θεμελιωδών Ελευθεριών». Το άρθρο 8 αναφερόταν στο δικαίωμα σεβασμού της

ιδιωτικής και οικογενειακής ζωής και αποτέλεσε ουσιαστικά το σημαντικότερο υπερεθνικό νομοθετικό κείμενο για την προστασία της ιδιωτικότητας με αντίκτυπο στον ευρωπαϊκό χώρο (Συμβούλιο της Ευρώπης, 1950). Αποτελεί ουσιαστικά το βασικό άξονα γύρω από τον οποίο περιστρέφεται η Ενωσιακή νομοθεσία, η οποία αναπτύσσεται εκτενέστερα στο επόμενο κεφάλαιο. Επίσης, το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει συμβάλλει αποφασιστικά με τη νομολογία στην αναγνώριση της προστασίας των προσωπικών δεδομένων και στην ερμηνευτική προσέγγιση της έννοιας της ιδιωτικότητας. Πρόκειται ουσιαστικά για το δικαίωμα κάθε ανθρώπου να μην καθίσταται πληροφοριακό αντικείμενο και να (συν)προσδιορίζει ο ίδιος ποιες πληροφορίες που τον αφορούν θα καταστούν γνωστές στο περιβάλλον.[1]

Η ανάγκη προάσπισης του δικαιώματος της προστασίας των προσωπικών δεδομένων εντάθηκε κατά τις δεκαετίες ’60 και ’70, όπου η πληροφορική και η γρήγορη εξέλιξη της τεχνολογίας άρχισε να κάνει αισθητή την εμφάνισή της. Η προστασία του ατόμου από την αυτόματη επεξεργασία των προσωπικών του πληροφοριών αντιμετωπίσθηκε για πρώτη φορά από τον περίφημο νόμο του ομόσπονδου κρατιδίου της Έσσης στη Γερμανία το 1970. Ακολούθησαν ο Σουηδικός νόμος του 1973, ο Ομοσπονδιακός νόμος της Γερμανίας το 1977 και οι νόμοι της Αυστρίας, Γαλλίας, Δανίας, Νορβηγίας (1978) και του Λουξεμβούργου (1979). Βασικός στόχος των νομοθεσιών αυτών, υπήρξε η προστασία της «πληροφοριακής ιδιωτικότητας» και του «πληροφοριακού αυτοκαθορισμού» των ατόμων, το δικαίωμά τους δηλαδή να αποφασίζουν τα ίδια για τη συλλογή, διάδοση και τη γνωστοποίηση σε τρίτους των σχετικών με αυτά πληροφοριών. Στα πλαίσια αυτά, οι σχετικές εθνικές νομοθεσίες περιόριζαν τη δυνατότητα επεξεργασίας των προσωπικών πληροφοριών των ατόμων σε σκοπούς σαφώς προκαθορισμένους, οι οποίοι όχι μόνο θα έπρεπε να είναι γνωστοί στο υποκείμενο των προσωπικών δεδομένων αλλά θα έπρεπε, επιπλέον, να έχουν γίνει και ρητά αποδεκτοί από αυτό. Άλλωστε, συνειδητοποιώντας το πρόβλημα αυτό και οι Διεθνείς Οργανισμοί είχαν από νωρίς

[1] 1. «Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του». 2. «Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων» (Συμβούλιο της Ευρώπης, 1950).

αναλάβει σημαντικές πρωτοβουλίες, είτε υπό τη μορφή μη δεσμευτικών, κατευθυντήριων οδηγιών και συστάσεων, όπως εκείνες του ΟΟΣΑ, είτε υπό τη μορφή διεθνών συμβάσεων, όπως η εξαιρετικά σημαντική Σύμβαση 108 που υπογράφηκε στις 28.1.1981 του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Η Σύμβαση 108 ήταν το πρώτο διεθνές νομικά δεσμευτικό κείμενο στον τομέα της προστασίας των προσωπικών δεδομένων ενώ η κύρωσή της από το ελληνικό κοινοβούλιο έγινε αρκετά χρόνια αργότερα με τον Ν.2068/1992. (Ιγγλεζάκης, 2004). Η εν λόγω Σύμβαση λοιπόν, η οποία, στη συνέχεια, κωδικοποίησε τις αρχές εκείνες που αποτελούσαν το «σκληρό πυρήνα» της προστασίας των δεδομένων προσωπικού χαρακτήρα των ατόμων (όπως π.χ. την ποιότητα της επεξεργασίας, τα ευαίσθητα δεδομένα, κ.λπ.), έδωσε το έναυσμα για τη δημιουργία μιας νέας, «δεύτερης γενιάς» νομοθετημάτων. Έτσι, αρκετές χώρες προέβησαν στη ψήφιση ειδικών νομοθεσιών ενώ άλλες προχώρησαν σε τροποποίηση της υπάρχουσας νομοθεσίας τους, αναθεωρώντας τις αντιλήψεις των νομοθετημάτων της «πρώτης γενιάς». Το 1990, ο Ο.Η.Ε. εξέδωσε κατευθυντήριες οδηγίες σε σχέση με την προστασία των ηλεκτρονικών βάσεων δεδομένων, περιλαμβάνοντας για πρώτη φορά και διατάξεις για την εποπτεία και για τα συστήματα κυρώσεων από τις παραβάσεις, γεγονός που αποδεικνύει την μετέπειτα συνειδητοποίηση της ανάγκης ορθής εφαρμογής των κανόνων προστασίας προσωπικών δεδομένων.

2.3 Η Ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων

Ο όρος περί προστασίας προσωπικών δεδομένων, αναφέρθηκε για πρώτη φορά στο άρθρο 6 της Συνθήκης για την Ευρωπαϊκή Ένωση, στο άρθρο 8 της Ευρωπαϊκής Σύμβασης των δικαιωμάτων του ανθρώπου και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Ειδικότερα ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ, στο άρθρο 8, εκτός από το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα το οποίο αποτυπώθηκε και στο άρθρο 16 (πρώην άρθρο 286 ΣΕΚ) της Συνθήκης για τη λειτουργία της Ευρωπαϊκής

Ένωσης[2], περιλαμβάνει κύριες αρχές, όπως τη νομιμότητα που πρέπει να διέπει την επεξεργασία των δεδομένων τους, να είναι θεμιτός ο λόγος της επεξεργασίας, καθώς και ότι κάθε πρόσωπο έχει δικαίωμα πρόσβασης στα «συλλεχθέντα δεδομένα» που τον αφορούν και ότι τη διασφάλιση αυτών την αναλαμβάνει ανεξάρτητη Αρχή[3].

Η πρώτη ολοκληρωμένη αναφορά για την προστασία των δεδομένων προσωπικού χαρακτήρα, έγινε με την Οδηγία 95/46/ΕΚ, «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», αν και πολύ πιο εξειδικευμένη και λεπτομερειακή, βασίσθηκε, ουσιαστικά, στη Σύμβαση του Συμβουλίου της Ευρώπης. (Σωτηρόπουλος , 2006) Η ψήφιση της Οδηγίας 95/46/ΕΚ σηματοδότησε την «τρίτη γενιά» νομοθετημάτων. Ωστόσο, αποτέλεσε και αντικείμενο κριτικής, για τις γενικές και ασαφείς ρυθμίσεις που περιέχει, με τρόπο ώστε να δίνει την ευκαιρία στον εθνικό νομοθέτη του κάθε κράτους να έχει ένα μεγάλο περιθώριο διακριτικής ευχέρειας, η οποία μάλιστα αξιοποιήθηκε και από τον Έλληνα νομοθέτη προς περαιτέρω ενίσχυση της προστασίας του πολίτη (Ιγγλεζάκης, 2004).

Με τις ρυθμίσεις της γενικής Οδηγίας 95/46/ΕΚ επιδιώκεται, αφενός η εξασφάλιση της προστασίας θεμελιωδών δικαιωμάτων των φυσικών προσώπων, με κυριότερο εκείνο της προστασίας της ιδιωτικής ζωής αυτών από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αφετέρου δε η διασφάλιση της απρόσκοπτης διασυνοριακής ροής προσωπικών δεδομένων μεταξύ των κρατών μελών σε τομείς της

[2] 15 Άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ 2012/C 326:
«1. Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν.
2. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών» (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2012).
[3] Χάρτης θεμελιωδών δικαιωμάτων της ΕΕ 2000/C 364, άρθρο 8 (Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, 2000):
«1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.
2.Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.
3.Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής».

οικονομικής, διοικητικής και κοινωνικής δραστηριότητας. Έτσι, η Οδηγία αποσκοπεί στην εναρμόνιση των εθνικών νομοθεσιών στο ζήτημα της προστασίας των δεδομένων προσωπικού χαρακτήρα ούτως ώστε να εξαλειφθούν τα εμπόδια στην κυκλοφορία των δεδομένων αυτών, ενώ παράλληλα επιδιώκει να εξασφαλιστεί η ελεύθερη ροή των δεδομένων. Περαιτέρω, στόχος της επιδιωκόμενης εναρμόνισης είναι η κατοχύρωση ενός υψηλού επιπέδου προστασίας των προσωπικών δεδομένων των ατόμων στην κοινότητα. Η Οδηγία 95/46/ΕΚ είναι τεχνολογικά ουδέτερη και ως εκ τούτου δύναται να εφαρμοστεί στο διαρκώς μεταβαλλόμενο τεχνολογικά περιβάλλον.

Αξίζει να τονιστεί ότι η Οδηγία 95/46/ΕΚ βρίσκει εφαρμογή, καταρχήν, όταν η επεξεργασία προσωπικών δεδομένων εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους (άρθρο 4 παρ. 1 περ. α'). Συνεπώς, δεν εμπίπτει στο πεδίο εφαρμογής του νόμου η επεξεργασία προσωπικών δεδομένων από παρόχους υπηρεσιών π.χ. κοινωνικής δικτύωσης που δεν έχουν εγκατάσταση στην επικράτεια κράτους μέλους της ΕΕ. Με την εν λόγω οδηγία διευκρινίστηκαν οι όροι «προσωπικά δεδομένα» και «επεξεργασία». Ειδικότερα:

Ως «**προσωπικά δεδομένα**» ορίζονται από το άρθρο 2 της Οδηγίας «όλες οι πληροφορίες που αφορούν κάποιο πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα». Επίσης, ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται «το πρόσωπο εκείνο που μπορεί να προσδιοριστεί άμεσα ή έμμεσα, ιδίως βάση αριθμού ταυτότητας ή βάση συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη». Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα αυτά ονομάζεται υποκείμενο των δεδομένων.

Ως «**ευαίσθητα**» χαρακτηρίζονται «τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα

προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα».

Η **«επεξεργασία»** ορίζεται ευρύτατα από την Οδηγία ως: «κάθε εργασία που πραγματοποιείται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση ή η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η εναρμόνιση, ο συνδυασμός καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή» (άρθρο 2 β'). Προκειμένου για την νόμιμη επεξεργασία ευαίσθητων δεδομένων απαιτείται γραπτή συγκατάθεση του υποκειμένου τους μόνο εφόσον ισχύει μία τουλάχιστον από τις εξαιρέσεις που ορίζει ο Νόμος 2472/1997 στο άρθρο 7 ενώ για την νόμιμη επεξεργασία των απλών προσωπικών δεδομένων αρκεί, σε πρώτη φάση, η προφορική συγκατάθεση, όταν συντρέχουν οι προϋποθέσεις που ορίζει ο Νόμος 2472/1997 στο άρθρο 5.

Ακόμη η Οδηγία εισάγει περαιτέρω ορισμένες πολύ σημαντικές αρχές που θα πρέπει να τηρούνται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ιδίως:

α) Την **αρχή του σκοπού**, σύμφωνα με την οποία τα δεδομένα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο, (άρθρο 6),

β) Την **αρχή της νομιμότητας** κατά την οποία θα πρέπει να τηρείται τουλάχιστον μία από τις διαζευκτικά αναγραφόμενες στο άρθρο 7 προϋποθέσεις, όπως π.χ. ότι το πρόσωπο στο οποίο αφορά η πληροφορία θα πρέπει να έχει δώσει τη ρητή συγκατάθεσή του για την επεξεργασία. Η συγκατάθεση μάλιστα αυτή θα πρέπει να είναι ελεύθερη, ρητή και να δίνεται από το υποκείμενο τον δεδομένων εν πλήρη επίγνωση (άρθρο 2 η').

γ**)** Την **αρχή της διαφάνειας και πληροφόρησης των υποκειμένων των δεδομένων** (άρθρα 10 και 12). Ως προς τα παρεχόμενα προς τα άτομα δικαιώματα, η Οδηγία αναγνωρίζει το δικαίωμα πρόσβασης, διόρθωσης και αντίταξης, που σημαίνει ότι τα πρόσωπα στα οποία αναφέρονται τα δεδομένα έχουν το δικαίωμα να αποκτούν αντίγραφα των υπό επεξεργασία δεδομένων που τα αφορούν, καθώς και το δικαίωμα να ζητούν διόρθωση των ανακριβών δεδομένων. Παρέχεται επίσης το δικαίωμα, στο

πρόσωπο στο οποίο αναφέρονται τα δεδομένα να αντιταχθεί στην επεξεργασία αυτών, εκτός αν στην εθνική νομοθεσία ορίζεται διαφορετικά. (Μήτρου , 2017)

Το 2002, η Ευρωπαϊκή Ένωση με την Οδηγία 2002/58/ΕΚ αντικατέστησε την Οδηγία 95/46/ΕΚ, για να συμπεριλάβει και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα με γνώμονα την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η αντικατάσταση αυτή είχε κριθεί αναγκαία από τον κοινοτικό νομοθέτη ενόψει των ραγδαίων τεχνολογικών εξελίξεων στον τομέα των τηλεπικοινωνιών και ιδίως εκείνων που είχαν επέλθει στον τομέα του Διαδικτύου. Έτσι, η Οδηγία 2002/58/ΕΚ περιέχει πιο εξειδικευμένες, αλλά και «τεχνολογικά ουδέτερες» ρυθμίσεις, και εφαρμόζεται στην επεξεργασία των προσωπικών δεδομένων στο χώρο των τηλεπικοινωνιών ανεξάρτητα από το μέσο που χρησιμοποιείται, συμπεριλαμβάνοντας σαφώς και τις υπηρεσίες Διαδικτύου. Ακόμα, η διάταξη του άρθρου 15 παρ. 1 της Οδηγίας παρείχε στα κράτη-μέλη την διακριτική ευχέρεια να λαμβάνουν νομοθετικά μέτρα που να επιτρέπουν την φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για λόγους, όπως η διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας και η πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρήσης του συστήματος ηλεκτρονικών επικοινωνιών.

Ωστόσο, υπέστη δριμεία κριτική και αποδοκιμάστηκε έντονα από τις ευρωπαϊκές Αρχές Προστασίας Προσωπικών Δεδομένων, από μη κυβερνητικές οργανώσεις, καθώς και από πολλά κράτη μέλη της ΕΕ. Στον απόηχο των αντιδράσεων αυτών και μετά από μακρές διαπραγματεύσεις και συζητήσεις η ΕΕ υιοθέτησε την Οδηγία 2009/136/ΕΚ, με την οποία τροποποιεί πέντε οδηγίες που συσχετίζονται με την ρύθμιση ηλεκτρονικών επικοινωνιών, μεταξύ των οποίων και την Οδηγία 2002/58/ΕΚ.

Πλέον, είναι αδιαμφισβήτητο ότι η Οδηγία 95/46/ΕΚ έχει πλέον ξεπεραστεί και χρήζει εκσυγχρονισμού ιδίως διότι οι ραγδαίες τεχνολογικές εξελίξεις έχουν αλλάξει πλήρως τον τρόπο παροχής των υπηρεσιών της κοινωνίας της πληροφορίας. Επίσης, δεν έτυχε ποτέ ενιαίας εφαρμογής σε όλα τα κράτη-μέλη, αφού πρόκειται για μία Οδηγία «ελάχιστης εναρμόνισης», προκαλώντας έτσι, σύμφωνα με την Επιτροπή, στρεβλώσεις του ανταγωνισμού μεταξύ των κρατών-μελών της, καθώς και ανασφάλεια δικαίου. Στο πλαίσιο αυτών των δεδομένων η Ευρωπαϊκή Επιτροπή

έδωσε, στη δημοσιότητα την από 25/1/2012 «Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αναφορικά με την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων και την ελεύθερη διακίνηση αυτών (Γενικός Κανονισμός Προστασίας Δεδομένων)».[4]

Στην πρόταση αυτή, καταγράφεται μεν η πρόθεση του Ευρωπαϊκού νομοθέτη να υπάρξει πλήρης εναρμόνιση της προστασίας προσωπικών δεδομένων στην ΕΕ, αποσκοπώντας δε στην παροχή αυξημένου επιπέδου προστασίας, ενώ γίνονται βήματα προς την κατεύθυνση μιας πιο συνεπούς αντιμετώπισης των ζητημάτων προστασίας προσωπικών δεδομένων ειδικά στις υπηρεσίες κοινωνικής δικτύωσης. Το πλέον καινοτόμο όμως σημείο της είναι ότι προβαίνει στην αναγνώριση ενός «δικαιώματος στη λήθη», το οποίο δεν περιλαμβάνει μόνο το δικαίωμα του ατόμου να ζητήσει την διαγραφή των προσωπικών του δεδομένων και τη μη περαιτέρω διάδοσή τους, αλλά επιπλέον το δικαίωμα να ζητήσει από τρίτους την διαγραφή των παραπομπών σε δεδομένα (άρθρο 17 της Πρότασης).

Πιο πρόσφατα, η Ευρωπαϊκή Ένωση εξέδωσε τον Κανονισμό 2016/679 (GDPR) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και την κατάργηση της Οδηγίας 95/46/ΕΚ ο οποίος θα αναπτυχθεί εκτενέστερα στο Κεφάλαιο 3 της παρούσης εργασίας.

Αξίζει να σημειωθεί πως η Ευρωπαϊκή Ένωση εξέδωσε δύο ακόμα Οδηγίες, την Οδηγία 2016/680 και την Οδηγία 2016/681. Η πρώτη σχετίζεται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ενώ η δεύτερη αφορά τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

[4]Η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

Ουσιαστικά, όπως τονίζει και ο ιστορικός **Yuval Harari** σε πρόσφατη ομιλία του στο **World Economic Forum Annual Meeting** τον Ιανουάριο του 2018, ο Κανονισμός αποτελεί μια χαρακτηριστική περίπτωση εκ των υστέρων ρύθμισης, όπου ο νομοθέτης έρχεται να θεραπεύσει και όχι να προλάβει, καθώς η τεχνολογία προπορεύεται κατά πολύ του δικαίου, αλλά και ίσως της ηθικής.[5]

2.4 Η Ελληνική νομοθεσία περί προστασίας προσωπικών δεδομένων

Ο βασικότερος νόμος ο οποίος αφορά τα προσωπικά δεδομένα και πρώτος για την Ελληνική νομοθεσία είναι ο 2472/1997. Ο νόμος αυτός θεσπίζει τις προϋποθέσεις υπό τις οποίες μπορεί να γίνει η επεξεργασία των προσωπικών δεδομένων με τρόπο τέτοιο ώστε να προστατεύονται τα πρόσωπα στα οποία ανήκουν τα δεδομένα. Οι διατάξεις του νόμου αυτού πρέπει να εφαρμόζονται τόσο στις περιπτώσεις πλήρους αυτοματοποιημένης επεξεργασίας όσο και σε περιπτώσεις εν μέρει αυτοματοποιημένης διαδικασίας. Αυτό είναι ιδιαίτερα σημαντικό γιατί στην χώρα μας τα συστήματα βρίσκονται ακόμα σε μεταβατικό στάδιο. Μέχρι και σήμερα περνάνε από το πατροπαράδοτο χαρτί στον ηλεκτρονικό υπολογιστή οπότε πολλές φορές οι μέθοδοι επεξεργασίας απλής και αυτοματοποιημένης επεξεργασίας μπλέκονται.

Ειδικότερα ο νόμος θεσπίζει αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας, προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθέμενων δικαιωμάτων και συμφερόντων, και αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (Άρθρο 4). Εκεί ανευρίσκονται οι αρχές που πρέπει να διέπουν την ποιότητα των δεδομένων και οι οποίες πρέπει να ακολουθούνται κατά τον έλεγχο της νομιμότητας της επεξεργασίας. Είναι απόλυτα δεσμευτικές και αποτελούν κανόνες αναγκαστικού δικαίου από τους οποίους δεν μπορεί να παρεκκλίνει η ιδιωτική βούληση.

Στο άρθρο 7 μπαίνουν οι αρχές που αφορούν την επεξεργασία των ευαίσθητων προσωπικών δεδομένων, ενώ η προσθήκη του άρθρου 7Α όπου αναφέρονται όλες οι περιπτώσεις όπου ο υπεύθυνος επεξεργασίας δεν είναι υποχρεωμένος να λάβει άδεια

[5] Πηγή: https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/sessions/a0Wb000000AlH77EAF

για την επεξεργασία, έρχεται να συμπληρώσει το άρθρο 7 του νόμου[6].Για τα ευαίσθητα δεδομένα θεσπίζεται ως γενικός κανόνας η απαγόρευση της συλλογής και επεξεργασίας τους. Ωστόσο, κατά την παρ. 2 επιτρέπεται κατ' εξαίρεση η συλλογή και επεξεργασία ευαίσθητων δεδομένων εάν πληρούνται οι ουσιαστικές προϋποθέσεις που ορίζονται δεσμευτικά από το νόμο και, μόνο κατόπιν αδείας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Πιο συγκεκριμένα η συλλογή και επεξεργασία ευαίσθητων δεδομένων επιτρέπεται μόνο κατ' εξαίρεση και όταν συντρέχουν οι περισσότερες από τις ακόλουθες προϋποθέσεις:

1) Να έχει συγκατατεθεί έγγραφο στο υποκείμενο, εκτός εάν η συγκατάθεση έχει αποσπαστεί με τρόπο που αντίκειται στο νόμο ή στα χρηστά ήθη

2) Η επεξεργασία είναι αναγκαία για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεση του.

3) Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση του δικαιώματος του ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

4) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που υπόκειται σε καθήκον εχεμύθειας, υπό τον όρο ότι είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

5) Η επεξεργασία εκτελείται από δημόσια αρχή και είναι αναγκαία είτε για λόγους εθνικής ασφάλειας είτε για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά την διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας, είτε για λόγους προστασίας της δημόσιας υγείας, είτε για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών. Περαιτέρω, ο Έλληνας νομοθέτης κάνοντας χρήση της δυνατότητας που παρέχει η παρ. 4 άρθρο 8 της Οδηγίας 95/46/ΕΚ στα κράτη μέλη, προσέθεσε στον σχετικό κατάλογο της παρ. 2 άρθρο 8 της Οδηγίας δύο ακόμα εξαιρέσεις επιτρέποντας την επεξεργασία προσωπικών δεδομένων και όταν:

[6] ΚΕΦΑΛΑΙΟ Β΄- ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ Ν.2472/1997

6) Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς, υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

7) Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημόσιου λειτουργήματος ή την διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος.

Το κεφάλαιο Γ του παρόντος νόμου[7] αναφέρεται στα δικαιώματα του υποκειμένου απέναντι στην επεξεργασία καθώς και στην απονομή δικαιωμάτων στα πρόσωπα ώστε να είναι σε θέση να προστατέψουν τα δικαιώματα και συμφέροντά τους. Ενώ το κεφάλαιο Δ αφορά την Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα που θα δούμε στην συνέχεια. Ορίζει με σαφήνεια την σύνθεσή της αλλά και τις αρμοδιότητές της. Τέλος ο νόμος κλείνει με τις κυρώσεις που θα έχει κάποιος αν παραβιάσει τις διατάξεις περί δεδομένων προσωπικού χαρακτήρα[8]

Το 2006 ψηφίστηκε ο νόμος 3471/2006, όπου αφορά την προστασία δεδομένων προσωπικού χαρακτήρα στης ηλεκτρονικές επικοινωνίες. Ουσιαστικά αποτελεί την ενσωμάτωση της Ευρωπαϊκής Οδηγίας 2002/58/ΕΚ στην Ελληνική νομοθεσία. Ο Ν. 3471/2006 τροποποιήθηκε αρχικά από το Ν.3917/2011 που αφορά την διατήρηση των δεδομένων της επεξεργασίας. Εδώ έστω και με πέντε χρόνια καθυστέρηση έχουμε την ενσωμάτωση της Ευρωπαϊκής οδηγίας 2006/24/ΕΚ σχετικά με την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών.

Αξιοσημείωτο είναι ότι ο Έλληνας νομοθέτης εκμεταλλευόμενος τις υπό της ελάχιστης εναρμόνισης Οδηγίας 95/46/ΕΚ παρεχόμενες δυνατότητες και διακριτικές ευχέρειες, ενίσχυσε σε σημαντικό βαθμό την προστασία των πολιτών. Επομένως, ο Ν. 2472/1997 δε συνιστά πιστή μεταφορά της Οδηγίας στο εθνικό νομικό μας πλαίσιο, καθώς ο Έλληνας νομοθέτης απέκλινε σε ορισμένες διατάξεις τις κοινοτικές ρυθμίσεις, αξιοποιώντας το περιθώριο που του παρείχε η Οδηγία. Το νομοθέτημα

[7] Άρθρα: 11-14
[8] www.dpa.gr Ν.2472/1997

αυτό λοιπόν, παρά τις όποιες επιμέρους ατέλειες του, μπορεί αβίαστα να χαρακτηριστεί ως προοδευτικό και ικανό να προσφέρει επαρκή προστασία της ιδιωτικότητας και του «πληροφοριακού αυτοπροσδιορισμού» στα άτομα. (Παναγοπούλου , 2017)

Παρακάτω ακολουθεί ένα σχήμα όπου παρουσιάζονται κατά χρονολογική σειρά τόσο τα ευρωπαϊκά όσο και τα ελληνικά νομοθετήματα για την προστασία των προσωπικών δεδομένων, όπως εμφανίζονται στην διαδικτυακή σελίδα της «Αρχής Προστασίας Προσωπικών Δεδομένων».

Δεδομένα προσωπικού χαρακτήρα «Ειδικών κατηγοριών» ή «Ευαίσθητα» προσωπικά δεδομένα: αυτά που παρέχουν πληροφορίες για		
Οδηγία 95/46/ΕΚ (άρθρο 8)	**Νόμος 2472/1997** (άρθρο 2)	**Κανονισμός 2016/679** (άρθρο 9)
φυλετική ή εθνική καταγωγή	φυλετική ή εθνική προέλευση	φυλετική ή εθνοτική καταγωγή
πολιτικά φρονήματα	πολιτικά φρονήματα	πολιτικά φρονήματα
θρησκευτικές ή φιλοσοφικές πεποιθήσεις	θρησκευτικές ή φιλοσοφικές πεποιθήσεις	θρησκευτικές ή φιλοσοφικές πεποιθήσεις
συμμετοχή σε συνδικαλιστικές οργανώσεις	συμμετοχή σε συνδικαλιστική οργάνωση	συμμετοχή σε συνδικαλιστική οργάνωση
υγεία	υγεία	υγεία
σεξουαλική ζωή	ερωτική ζωή	σεξουαλική ζωή
	κοινωνική πρόνοια	
	ποινικές διώξεις ή καταδίκες	
	συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις	
		γενετικά δεδομένα
		βιομετρικά δεδομένα
		γενετήσιο προσανατολισμό

Εικόνα 1: Τα ευαίσθητα προσωπικά δεδομένα όπως αναφέρονται στην ευρωπαϊκή και στην ελληνική νομοθεσία. Πηγή: www.dpa.gr

2.5 Η ελληνική εποπτική «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»

Όπως αναφέρει και η ίδια η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στην σελίδα της, «η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα». Η ύπαρξη ωστόσο των δικαιωμάτων κάνει πολλές φορές την ζωή κάποιων δύσκολη μιας που πρέπει να προσαρμόσουν τις ενέργειές τους κατά τρόπο τέτοιο ώστε να τα σεβαστούν. Κάτι τέτοιο συνήθως είναι χρονοβόρο και κοστοβόρο και δεν είναι λίγες οι φορές που προσπαθούν εντέχνως να παρακάμψουν αυτά τα δικαιώματα. Η Αρχή λοιπόν είναι εδώ για να μπορεί να στηρίξει τον πολίτη στην διεκδίκηση του δικαιώματος αυτού και να το διαφυλάξει όσο είναι δυνατόν.

Πολλά προσωπικά δεδομένα υπάρχουν πλέον σε βάσεις δεδομένων ηλεκτρονικά. Συνεπώς πέρα από το δικαίωμα που έχει κάποιος να μην τα μοιραστεί αυτά, έπρεπε να θεσπιστεί και το δικαίωμα να μην έχει κάποιος πρόσβαση στον χώρο που αυτά είναι αποθηκευμένα. Έτσι ο Έλληνας νομοθέτης με το άρθρο 9 του συντάγματος ορίζει πως «Καθένας έχει δικαίωμα προστασίας από την συλλογή δεδομένων όπως το σύνταγμα ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται πλέον από μια ανεξάρτητη Αρχή που συγκροτείται και λειτουργεί σύμφωνα με τα όσα ορίζει ο νόμος». Η αρχή στην οποία αναφέρεται είναι η «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα».

Η ΑΠΔΠΧ όπως γράφεται για συντομία, είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή, η οποία ιδρύθηκε με τον 2472/1997 και ουσιαστικά είναι η ενσωμάτωση της Οδηγίας 95/46/ΕΚ της Ευρωπαϊκής Ένωσης. Η «Αρχή» κατά το άρθρο 15 «δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας. Η Αρχή υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα».

Ως αποστολή της Αρχής ορίζεται η προστασία των προαναφερθέντων προσωπικών και ευαίσθητων δεδομένων και της ιδιωτικής ζωής του ατόμου στην Ελλάδα. Σκοπός της Αρχής είναι να προστατεύει τον Έλληνα πολίτη από την παράνομη επεξεργασία των δεδομένων του αλλά και να τον βοηθάει σε περίπτωση που αυτά παραβιαστούν. Ταυτόχρονα η Αρχή καθοδηγεί και υποστηρίζει του

υπευθύνους επεξεργασίας δεδομένων, προκειμένου να ολοκληρώσουν την επεξεργασία που αποτελεί την δουλειά τους με τρόπο που να συμβαδίζει με τα όσα ορίζονται στο νόμο.

Η Αρχή είναι επταμελής και έχει έναν πρόεδρο ο οποίος είναι, τουλάχιστον, δικαστικός λειτουργός του Συμβουλίου της Επικρατείας. Η θητεία των μελών είναι τέσσερα έτη και υπάρχει δυνατότητα ανανέωσης μόνο για μία φορά. Η Αρχή επίσης διαθέτει και μία Γραμματεία η οποία έχει τρία τμήματα το τμήμα Ελεγκτών, το τμήμα Επικοινωνίας και το τμήμα Διοικητικών και Οικονομικών υποθέσεων. Ενώ τέλος οι αρμοδιότητες της αρχής χωρίζονται σε:

- Εποπτικές και ελεγκτικές εκδίδει δηλαδή οδηγίες, καλεί και επικουρεί τα επαγγελματικά σωματεία στην κατάρτιση κωδικών δεοντολογίας και απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και δίνει κατά την κρίση της δημοσιότητα σε αυτές

- Αποφασιστικές και συμβουλευτικές όπου αποφασίζει ή όχι για τη χορήγηση αδειών επεξεργασίας για την συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων, για τη διασύνδεση αρχείων όταν αφορούν ευαίσθητα δεδομένα και για τη διαβίβαση δεδομένων προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση

- Καθώς και σε νομοθετικές και γνωμοδοτικές όπου εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο Νόμος. Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα και εξετάζει αιτήσεις υπευθύνων επεξεργασίας με τις οποίες ζητείται ο έλεγχος και η νομιμότητα της επεξεργασίας.

Η Αρχή Προστασίας Προσωπικών Δεδομένων, κατέχει, όπως προαναφέρθηκε και δική της διαδικτυακή σελίδα όπου προσφέρει ένα σύνολο υπηρεσιών τόσο προς τους πολίτες όσο και προς τους υπεύθυνους επεξεργασίας. Οι πολίτες λοιπόν αρχικά μπορούν να καταθέσουν κάποια καταγγελία ή προσφυγή σχετικά με κάποια παραβίαση των δικαιωμάτων τους. Έπειτα μπορούν να υποβάλουν ερωτήματα και αιτήσεις για γνωμοδότηση. Επίσης στην επιτροπή οφείλει να απευθυνθεί κάποιος ο οποίος θέλει να αιτηθεί πρόσβαση στα δεδομένα που τον αφορούν. Τέλος ο πολίτης μπορεί να αιτηθεί να υπαχθεί στο άρθρο 13 ώστε να μην περιλαμβάνεται σε καταλόγους τηλεφωνικών πωλήσεων και προωθητικών ενεργειών αλλά και να ενημερώνεται από την αρχή για την εξέλιξη των υποθέσεών του.

Αντίστοιχα για τους υπεύθυνους επεξεργασίας η πύλη προσφέρει δυνατότητες όπως η χορήγηση της λίστας με τους πολίτες που υπάγονται στο άρθρο 13, ενώ οι υπεύθυνοι επεξεργασίας μπορούν να απευθύνουν οποιοδήποτε ερώτημα αφορά την επεξεργασία προς την αρχή αλλά και τις γνωστοποιήσεις για τις επεξεργασίες. Τέλος και αυτοί ενημερώνονται από την Αρχή για τις υποθέσεις στις οποίες εμπλέκονται.

Ο υπεύθυνος επεξεργασίας ενδέχεται να είναι ταυτόχρονα και «εκτελών» την επεξεργασία. Ο «εκτελών την επεξεργασία», εφόσον βεβαίως δεν ταυτίζεται με τον υπεύθυνο επεξεργασίας, ορίζεται από το νόμο ως «οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός».

Κάθε υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί στην Αρχή την επεξεργασία προσωπικών δεδομένων που πραγματοποιεί, εκτός αν εμπίπτει σε μία από τις περιπτώσεις του άρθρου 7Α του Ν. 2472/1997. Η Αρχή καταχωρεί τη γνωστοποίηση σε ειδικό μητρώο.

Όταν η επεξεργασία αφορά ευαίσθητα δεδομένα, ο υπεύθυνος επεξεργασίας μπορεί να την πραγματοποιήσει μόνο μετά από άδεια της Αρχής, η οποία χορηγείται με ειδικούς όρους και προϋποθέσεις. Άδεια επίσης μπορεί να απαιτείται για τη διαβίβαση δεδομένων σε χώρα εκτός Ε.Ε., καθώς και για τη διασύνδεση αρχείων.

Περαιτέρω, εξειδικευμένη αναφορά γίνεται από τον Έλληνα νομοθέτη στην διασύνδεση, η οποία αποτελεί μια μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας, ή που τηρούνται από τον ίδιο υπεύθυνο για άλλο σκοπό. Ο νόμος καθιερώνει καταρχήν σύστημα γνωστοποίησης κάθε διασύνδεσης στην Αρχή Προστασίας Προσωπικών Δεδομένων και, παράλληλα, σύστημα προηγούμενης άδειας της Αρχής (άδεια διασύνδεσης) εάν ένα τουλάχιστον από τα αρχεία ή τις επεξεργασίες που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα.

Τέλος, ο νόμος παρέχει στην Αρχή τη δυνατότητα επιβολής διοικητικών (άρθρο 21), ποινικών (άρθρο 22) και αστικών (άρθρο 23) κυρώσεων.

Ειδικότερα, όσον αφορά τις διοικητικές κυρώσεις, αυτές επιβάλλονται από την Αρχή στους υπευθύνους επεξεργασίας ή στους τυχόν εκπροσώπους τους και ξεκινούν, στις πιο απλές περιπτώσεις από μία απλή προειδοποίηση με αποκλειστική προθεσμία για άρση της παράβασης, εκτείνονται σε πρόστιμα και δύνανται να φτάσουν έως την οριστική ανάκληση της άδειας και την καταστροφή του αρχείου ή τη διακοπή της επεξεργασίας των σχετικών δεδομένων.

Ποινικές κυρώσεις επιβάλλονται ιδίως στην περίπτωση μη γνωστοποίησης αρχείου, λειτουργίας αρχείου με ευαίσθητα δεδομένα χωρίς άδεια κ.α., καθώς και στην περίπτωση μη συμμόρφωσης προς τις αποφάσεις της Αρχής. Οι ποινικές κυρώσεις κυμαίνονται από φυλάκιση ενός μέχρι 10 έτη και χρηματική ποινή.

Το πλέγμα των προβλεπόμενων από το νόμο κυρώσεων ολοκληρώνεται με τις αστικές κυρώσεις, δηλαδή την αστική ευθύνη των υπαίτιων για κάθε ζημία περιουσιακής ή μη φύσεως.

Μία από τις πιο πρόσφατες γνωμοδοτήσεις της Αρχής μόλις την 1η το 2017 αφορά το ηλεκτρονικό εισιτήριο που θέλησε να θεσπίσει ο ΟΑΣΑ στην Αθήνα. Ενώ ο οργανισμός ανακοίνωσε την ισχύ του ηλεκτρονικού εισιτηρίου η Αρχή πάγωσε την διαδικασία.

Η υπόθεση αυτή αφορά την αρχή καθώς απαιτεί ταυτοποίηση των επιβατών. Κάποιοι από αυτούς μετακινούνται με μειωμένο ή και μηδενικό κόμιστρο πράγμα το οποίο αντικατοπτρίζει την οικονομική τους κατάσταση ορισμένες φορές. Επίσης για την έκδοση του εισιτηρίου απαιτείται να δοθούν κάποια προσωπικά δεδομένα όπως ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), το ονοματεπώνυμο, η διεύθυνση, η ημερομηνία γέννησης, ο αριθμός τηλεφώνου, το ηλεκτρονικό ταχυδρομείο αλλά και φωτογραφία σε ψηφιακή μορφή.

Η Αρχή θεωρεί πως αρχικά καταπατάται η αρχή της αναλογικότητας καθώς τα δεδομένα που συλλέγονται και επεξεργάζονται είναι πάρα πολλά. Γι’ αυτό και ζήτησε από τον οργανισμό να αιτιολογήσει την αναγκαιότητα όλων όσων θέλει να θεσπίσει προκειμένου να δώσει η Αρχή το πράσινο φως για τα ηλεκτρονικά εισιτήρια.

Τέλος αξίζει να σημειωθεί, πως ο Γενικός Κανονισμός, που θα αναλυθεί εκτενέστερα στο επόμενο κεφάλαιο, στα άρθρα 51 έως 67 επανακαθορίζει τους κανόνες για την σύσταση των εθνικών εποπτικών αρχών τις προϋποθέσεις

λειτουργίας τους, τις αρμοδιότητες, τα καθήκοντα και τις εξουσίες τους καθώς και τις διαδικασίες που πρέπει να ακολουθήσουν στους τομείς της συνεργασίας και της συνεκτικότητας, ορίζοντας τρεις νέες κατηγορίες εξουσιών που οφείλει να διαθέτει:

- ✓ Εξουσίες έρευνας, με μορφή ελέγχων, προβαίνει σε επανεξέταση πιστοποιήσεων, προειδοποιεί για «εικαζόμενη παράβαση», και έχει πρόσβαση σε δεδομένα και εγκαταστάσεις επεξεργασίας προσωπικών δεδομένων.
- ✓ Εξουσίες διορθωτικές, δηλαδή προειδοποιήσεις, επιπλήξεις, εντολές συμμόρφωσης και τήρησης των διατάξεων, εντολή κοινοποίησης στα υποκείμενα των παραβάσεων καθώς και περιορισμό ή απαγόρευση της επεξεργασίας.
- ✓ Εξουσίες συμβουλευτικές, όπως έκδοση γνώμης, παροχή διαπιστεύσεων φορέων πιστοποίησης, έγκριση τυποποιημένων συμβατικών ρητρών, έγκριση διοικητικών ρυθμίσεων αλλά και κατά παρέκκλιση έκδοση άδειας για επεξεργασία προσωπικών δεδομένων.

2.6 Σύνοψη

Μετά την σύντομη ιστορική αναδρομή σχετικά με την εξέλιξη των προσωπικών δεδομένων στη διάρκεια των ετών, φάνηκε η επιτακτική ανάγκη των νομοθετών να θεσπίσουν νέους νόμους και κανονισμούς για την όσο δυνατόν μεγαλύτερη διασφάλιση των προσωπικών δεδομένων των ανθρώπων. Οι παραδοσιακές θεσμικές ρυθμίσεις δεν φαίνονταν επαρκείς για την προστασία των ατόμων μέσα στα πλαίσια της εξελικτικά διαμορφούμενης κοινωνίας της πληροφορίας και επομένως απαιτούνταν ειδικές προστατευτικές ρυθμίσεις που να παρέχουν μια πιο αποτελεσματική προστασία στα υποκείμενα των προσωπικών αυτών δεδομένων. Έτσι, αρχίζουν να κάνουν την εμφάνισή τους κατά τις δεκαετίες του 1970 (νομοθεσίες «πρώτης γενιάς») και 1980 (νομοθεσίες «δεύτερης γενιάς») σημαντικά ευρωπαϊκά και μετέπειτα εθνικά νομοθετήματα περί προστασίας των προσωπικών δεδομένων. Στη χώρα μας, ιδιαίτερο ρόλο στη διαμόρφωση «κουλτούρας» για την προστασία των προσωπικών δεδομένων, διαδραμάτισε όπως παρουσιάστηκε στο κύριο μέρος, ο Ν. 2472/1997, όπου θέσπισε νέες αρχές νομιμότητας και επεξεργασίας των προσωπικών δεδομένων των ατόμων.

Ακόμη η υποχρεωτική ίδρυση της «Αρχής Προστασίας Προσωπικών Δεδομένων», καθώς και η ραγδαία εξέλιξη της τεχνολογίας της πληροφορικής και

των διαδικτυακών μέσων, έκανε ακόμη πιο επιτακτική την ανάγκη για εκσυγχρονισμό των υφιστάμενων κανόνων της προστασίας των προσωπικών δεδομένων, με την υιοθέτηση ενός νέου ρυθμιστικού πλαισίου για την προστασία των προσωπικών δεδομένων, τόσο των φυσικών προσώπων, όσο και των οικονομικών οντοτήτων δημοσίων ή ιδιωτικών. Γίνεται τέλος πιο επιτακτική η ανάγκη, ώστε ο ρόλος της Αρχής από κυρίως γραφειοκρατικό να αλλάξει σε έντονα ελεγκτικό, που εκτός από δικαιώματα δημιουργεί και ευθύνες.

ΚΕΦΑΛΑΙΟ 3 : Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)

3.1 Εισαγωγή

Το νομοθετικό πλαίσιο που ρυθμίζει την προστασία των προσωπικών δεδομένων αποτελεί ήδη παρελθόν εξαιτίας της εκ βάθρων αλλαγής του. Η ραγδαία τεχνολογική εξέλιξη, η παγκοσμιοποίηση, η πρόσβαση στο διαδίκτυο με την χρήση ασύρματων μέσων, τα κοινωνικά δίκτυα, οι υπηρεσίες υπολογιστικών νεφών και εν γένει η χρήση του διαδικτύου στο πλαίσιο τόσο προσωπικών, όσο και επαγγελματικών δραστηριοτήτων και συμπεριφορών που οδηγούν στην δημιουργία «δεξαμενών» προσωπικών δεδομένων, η παγκοσμιοποίηση καθώς και η διαβίβαση και ανταλλαγή δεδομένων μεταξύ διαφορετικών κρατών, κατέστησαν την Οδηγία 95/46/ΕΚ ξεπερασμένη.

Είκοσι χρόνια μετά τη θέση σε ισχύ του Ν. 2472/1997 για την προστασία των προσωπικών δεδομένων, ένας νέος Κανονισμός έρχεται να επαναπροσδιορίσει άμεσα, χωρίς άλλη ειδική νομοθεσία τις υποχρεώσεις όσων επεξεργάζονται προσωπικά δεδομένα στην Ε.Ε.

Στις 25.1.2012, η Ευρωπαϊκή Επιτροπή πρότεινε τη μεταρρύθμιση των κανόνων προστασίας προσωπικών δεδομένων στην ΕΕ. Μετά από πολυετείς συζητήσεις και διαβουλεύσεις, το Συμβούλιο ενέκρινε τη θέση του σε πρώτη ανάγνωση στις 8.4.2016 και στις 14.4.2016, ο Κανονισμός και η Οδηγία (ΕΕ) 2016/680 εγκρίθηκαν από το

Ευρωπαϊκό Κοινοβούλιο. Στις 27.4.2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) που αποτελεί το κύριο νομοθέτημα της νέας δέσμης κανόνων. Κάθε επιχείρηση που είναι εγκατεστημένη στην Ευρωπαϊκή Ένωση, ή που είναι εγκατεστημένη εκτός Ευρωπαϊκής Ένωσης και χειρίζεται προσωπικά δεδομένα τα οποία αφορούν σε άτομα που βρίσκονται εντός της Ευρωπαϊκής Ένωσης, είναι υποχρεωμένη να συμμορφωθεί πλήρως στις επιταγές του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), ο οποίος στις 4.5.2018 δημοσιεύτηκε στην Επίσημη Εφημερίδα της ΕΕ και τέθηκε σε εφαρμογή την 25η Μαΐου 2018

Πρακτικά λοιπόν, βρισκόμαστε ήδη στο χρονικό σημείο όπου θα λέγαμε ότι έχει αρχίσει η αντίστροφη μέτρηση για μια νέα εποχή, με αυξημένες μεν ‘’γραφειοκρατικές’’ και άλλες υποχρεώσεις και απαιτούμενη τυπολογία από πλευράς επιχειρήσεων, η οποία όμως μακροπρόθεσμα στοχεύει να εξισορροπήσει μεταξύ του δικαιώματος της προστασίας των προσωπικών δεδομένων από τη μία πλευρά και του δικαιώματος στην πληροφόρηση, διαφάνεια και δημόσια ασφάλεια από την άλλη, με τρόπο που να προάγει την ελεύθερη και ανεμπόδιστη οικονομική ανάπτυξη και επιχειρηματική δραστηριότητα. Η προάσπιση της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων, είναι βασικό ζητούμενο και αποτελεί πρόκληση του νέου Κανονισμού που φιλοδοξεί να αντιμετωπίσει τη σύγχρονη πραγματικότητα των εφαρμογών, των έξυπνων συσκευών, των αισθητήρων και κάθε λογής τεχνολογίας που επικοινωνεί με το διαδίκτυο και με απομακρυσμένους υπολογιστές.

Στο παρόν κεφάλαιο, αναλύονται όλα τα νέα δεδομένα, οι ορισμοί και οι υποχρεώσεις που φέρνει ο συγκεκριμένος Κανονισμός, με τους πολίτες και τις επιχειρήσεις να έχουν τον κυρίαρχο ρόλο στην αποδοχή των αλλαγών αυτών.

3.2 Ανάλυση περιεχομένου του GDPR

Από τις 25.5.2018 όλες οι επιχειρήσεις, οι οργανισμοί και οι κυβερνητικές υπηρεσίες που συλλέγουν, διατηρούν, επεξεργάζονται, αποθηκεύουν και χρησιμοποιούν προσωπικά δεδομένα (εργαζομένων, πελατών, προμηθευτών ή τρίτων) έχουν την υποχρέωση να εφαρμόζουν τις νέες διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR). Η προσαρμογή των

επιχειρήσεων αφορά νέα δικαιώματα που πρέπει να ικανοποιούν και νέες διαδικασίες που πρέπει να τηρούν, ενώ η μη συμμόρφωση προς τον Κανονισμό θα επιφέρει μεγάλα πρόστιμα σε όσους δεν λαμβάνουν τα απαραίτητα μέτρα.

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (EU GDPR 2016/679, στο εξής GDPR) προστατεύει τα φυσικά πρόσωπα από κινδύνους που σχετίζονται με την ανεξέλεγκτη -μέχρι πρότινος- επεξεργασία των προσωπικών τους δεδομένων. Θέτει αυστηρότερους κανόνες στους οργανισμούς, για να περιορίσει την ανεξέλεγκτη και αλόγιστη επεξεργασία προσωπικών δεδομένων και να μειώσει τους κινδύνους για τα φυσικά πρόσωπα. Απώτερος σκοπός είναι να δημιουργηθεί ένα ευρύτερο ασφαλές περιβάλλον, ίδιο σε όλα τα κράτη-μέλη της Ευρώπης, κάτω από μία ενιαία νομοθεσία, που θα προστατεύει αποτελεσματικά τα φυσικά πρόσωπα, ώστε να εξασφαλιστεί η ελεύθερη διακίνηση των προσωπικών δεδομένων μεταξύ των κρατών, δίχως κινδύνους για τα φυσικά πρόσωπα.

Ο νέος γενικός Κανονισμός διαρθρώνεται σε 11 κεφάλαια και αποτελείται από 99 άρθρα όπου περιλαμβάνονται αρκετές καινοτομίες.

Στο κεφάλαιο Ι Γενικές Διατάξεις διευρύνεται το εδαφικό πεδίο εφαρμογής, όπου ο Κανονισμός εφαρμόζεται σε δραστηριότητες εγκατάστασης του υπεύθυνου ή εκτελούντος την επεξεργασία στην ΕΕ, ακόμη και εάν η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται σε χώρα εκτός της ΕΕ. Επίσης, εφαρμόζεται σε δραστηριότητες εγκατάστασης του υπεύθυνου ή εκτελούντος την επεξεργασία εκτός ΕΕ, αλλά η επεξεργασία αφορά υποκείμενα δεδομένων που βρίσκονται εντός της ΕΕ. Αυτό σημαίνει ότι σχεδόν κάθε μεγάλη εταιρία παγκοσμίως θα πρέπει να αρχίσει να δουλεύει στη στρατηγική που θα ακολουθήσει για την εφαρμογή του Κανονισμού, ώστε να είναι έτοιμη μέχρι τον Μάιο που θα τεθεί σε ισχύ το GDPR. Επίσης επανακαθορίζεται ο ορισμός των δεδομένων προσωπικού χαρακτήρα περιλαμβάνοντας τις έννοιες δεδομένα θέσης και επιγραμμικά (on line) αναγνωριστικά στοιχεία ταυτότητας. Διατυπώνονται νέοι ορισμοί όπως ο περιορισμός της επεξεργασίας, η κατάρτιση προφίλ, η ψευδωνυμοποίηση, τα γενετικά και βιομετρικά δεδομένα.

Στο κεφάλαιο ΙΙ επικαιροποιούνται, προστίθενται και αναφέρονται συγκεκριμένα οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αναλυτικά, διατυπώνονται:

❖ **Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας** που επιβάλει την σύννομη, θεμιτή και με διαφανή τρόπο επεξεργασία αναφορικά με το υποκείμενο των δεδομένων.

❖ Η **αρχή του σκοπού** που εκπληρώνεται όταν η συλλογή και η επεξεργασία γίνονται με στόχο σαφή και καθορισμένο που δεν επιτρέπει την υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Μόνη επιτρεπτή εξαίρεση συνιστά η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας

❖ Η **αρχή ελαχιστοποίησης των δεδομένων** η οποία πρέπει να εφαρμόζεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια τήρησης αυτών και βάσει της οποίας τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως απαραίτητα αναφορικά με τους σκοπούς για τους οποίους εκτελείται η επεξεργασία.

❖ Η **αρχή της ακρίβειας** σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται ενώ το υποκείμενο θα πρέπει να έχει επαρκή ενημέρωση ως προς τα προσωπικά του δεδομένα τα οποία υφίστανται επεξεργασία. Παράλληλα, πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας

❖ Η **αρχή του περιορισμού της περιόδου αποθήκευσης**, δηλαδή την τήρηση των αρχείων των δεδομένων για όσο διάστημα χρειάζεται για την επίτευξη του σκοπού της επεξεργασίας. Εξαίρεση προβλέπεται στην περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και λαμβάνονται τα κατάλληλα οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

❖ Η **αρχή της ακεραιότητας και εμπιστευτικότητας** που καλεί για την υποβολή των δεδομένων σε επεξεργασία κατά τρόπο ώστε να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

❖ Η **αρχή της αναλογικότητας** που επιβάλλει να υπάρχει συνάφεια ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο αυτά συλλέγονται, καθώς

και να είναι τα δεδομένα αυτά πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού αυτού. Με τον τρόπο αυτό, η αρχή της αναλογικότητας οδηγεί πρακτικά στην ελαχιστοποίηση των τηρούμενων δεδομένων, αφού το πιθανότερο είναι πως οι προϋποθέσεις αυτές δεν ισχύουν για το σύνολο των δεδομένων που συλλέγονται από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία.

❖ Η **αρχή της λογοδοσίας** όπου ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, οφείλουν να συμμορφώνονται και να αποδεικνύουν ανά πάσα στιγμή τη συμμόρφωσή τους με τις ανωτέρω αρχές. Οι υποχρεώσεις τους δεν είναι προκαθορισμένες και σταθερές αλλά διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως ο κίνδυνος αυτός εκτιμάται ήδη πριν την έναρξη της επεξεργασίας, βάσει της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων.[9]

Οι νέες λοιπόν αρχές επιβάλλουν σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων ώστε οι διαδικασίες επεξεργασίας να καλύπτονται από νομιμότητα, αντικειμενικότητα και διαφάνεια. Τα δεδομένα πλέον διέπονται από την αρχή του περιορισμού του σκοπού, που σημαίνει πως τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να συλλέγονται για καθορισμένους ρητούς και νόμιμους σκοπούς και δεν θα υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Ελαχιστοποιεί τα δεδομένα ώστε να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, επιβάλλει την ακρίβεια και την επικαιροποίηση τους όταν αυτό κρίνεται αναγκαίο με τρόπο που να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων τα οποία είναι ή καθίστανται ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας. Τα δεδομένα διατηρούνται στην μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων δεδομένων αλλά και αποθηκεύονται μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας με τρόπο που να περιορίζεται η περίοδος αποθήκευσης.

Ο νέος Κανονισμός ενδυναμώνει τα δικαιώματα του υποκειμένου των δεδομένων, παρέχοντάς του μεγαλύτερο έλεγχο επί των προσωπικών του δεδομένων στο κεφάλαιο ΙΙΙ. Τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων και μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία

[9]Κατευθυντήριες Οδηγίες της Ομάδας Εργασίας 29 για την αρχή της διαφάνειας

απώλεια, καταστροφή ή φθορά με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέσων, αρχές που επιβάλλουν την ακεραιότητα, εμπιστευτικότητα και διαφάνεια. Περιλαμβάνει ειδικές προστατευτικές ρυθμίσεις για τα προσωπικά δεδομένα των παιδιών, δίνει το δικαίωμα στο υποκείμενο των δεδομένων να προβεί σε καταγγελία στην εποπτική αρχή καθώς επίσης και σε δικαστική προσφυγή και αποζημίωση.

Το εχέγγυο της αυξημένης προστασίας των προσωπικών δεδομένων αναλαμβάνει να εξασφαλίσει ένας νέος θεσμός που εισάγεται στο κεφάλαιο IV, αυτός του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer), ο οποίος θα πρέπει να ορίζεται σε αρκετές περιπτώσεις τόσο από τις επιχειρήσεις, όσο και από το Δημόσιο και ο οποίος θα κληθεί να αναλάβει το ρόλο του θεματοφύλακα των προσωπικών δεδομένων, καθώς με τις ειδικές επιστημονικές του γνώσεις στο αντικείμενο θα μπορεί να προλαμβάνει περιπτώσεις παραβίασης προσωπικών δεδομένων διασφαλίζοντας την ομαλή τήρηση των προϋποθέσεων του Κανονισμού. Ακόμη προτρέπετε η εκπόνηση και τήρηση κώδικα δεοντολογίας, η θέσπιση κανόνων πιστοποίησης, σφραγίδων και σημάτων προστασίας.

Ακολουθεί το κεφάλαιο VI όπου καθορίζονται οι αρμοδιότητες, τα καθήκοντα, οι εξουσίες των εποπτικών αρχών. Κατά την μελέτη των επιμέρους άρθρων, διαπιστώνεται ότι ουσιαστικά η εποπτική αρχή παρακολουθεί την εφαρμογή του παρόντος Κανονισμού, συμβάλλει στη συνεκτικότητά του και λειτουργεί ανεξάρτητα.

Ως αρχή ελέγχου έχει την δυνατότητα ελέγχου, διόρθωσης, αδειοδότησης, συμβουλευτικής και γνωστοποίησης στις δικαστικές αρχές παραβιάσεις του παρόντος Κανονισμού. Η Οδηγία 95/46/ΕΚ καθόριζε τη γενική υποχρέωση γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές, παρόλα αυτά ο περιορισμός αυτός δεν συνέβαλε στην βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα Ως αποτέλεσμα αυτού, ο νέος Κανονισμός δίνει τη δυνατότητα στο κάθε κράτος μέλος να νομοθετήσει την υποχρέωση ή μη αδειοδότησης από την εποπτική αρχή ακόμη και κατά την επεξεργασία δεδομένων ειδικών κατηγοριών (όπως γενετικά, βιομετρικά δεδομένα ή δεδομένα που αφορούν την υγεία). Επιπλέον, προκειμένου να διασφαλίζεται η ανεξαρτησία των δικαστικών αρχών κατά την άσκηση των δικαιοδοτικών τους αρμοδιοτήτων, οι εποπτικές αρχές δεν ελέγχουν πράξεις επεξεργασίας που διενεργούνται από τα δικαστήρια. Τέλος,

συστήνεται το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ως ανεξάρτητος φορέας το οποίο θα αντικαταστήσει την Ομάδα του άρθρου 29.

Σύμφωνα με το άρθρο 4 του νέου Κανονισμού, υπάρχουν δύο τύποι «χειριστών» δεδομένων:

1) Ο «**υπεύθυνος επεξεργασίας**», δηλαδή «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους»,

2) Ο «**εκτελών την επεξεργασία**», δηλαδή «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».

Ουσιαστικά ο νέος Κανονισμός επιβαρύνει με μεγαλύτερη νομική ευθύνη σε περίπτωση παραβίασης, τον «εκτελών την επεξεργασία», αφού οφείλει να διατηρεί και να επεξεργάζεται τα αρχεία των προσωπικών δεδομένων, παρέχοντας ένα μεγαλύτερο επίπεδο νομικής προστασίας από παραβιάσεις στον οργανισμό ή την επιχείρηση. Αυτές οι υποχρεώσεις είναι μια καινούρια παράμετρος που εισάγεται με τον GDPR.

Οι «υπεύθυνοι επεξεργασίας» θα είναι επίσης επιφορτισμένοι με την αρμοδιότητα να διασφαλίζουν ότι όλες οι συναλλαγές και επικοινωνίες με τους «εκτελούντες την επεξεργασία», είναι πλήρως εναρμονισμένες με τα όσα ορίζονται στον GDPR.

Τέλος, με το νέο Κανονισμό, κάθε Αρχή Ελέγχου, 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 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.

Συνεπώς, τα φυσικά πρόσωπα αλλά και πολύ περισσότερο οι οικονομικές οντότητες, θα πρέπει επιμελώς να προβούν σε όλες τις δέουσες ενέργειες για να ενημερωθούν, να προσαρμοστούν και να συμμορφωθούν με την νέα τάξη δεδομένων.

3.3 Η έννοια της συγκατάθεσης

Η έννοια της συγκατάθεσης, όπως χρησιμοποιείται στην οδηγία για την προστασία δεδομένων (οδηγία 95/46/ΕΚ) καθώς και της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, έχει εξελιχθεί. Το GDPR διευκρινίζει και εξειδικεύει περαιτέρω τις απαιτήσεις απόκτησης και απόδειξης έγκυρης συγκατάθεσης. Οι εν προκειμένω κατευθυντήριες γραμμές επικεντρώνονται σε αυτές τις αλλαγές, παρέχοντας πρακτική καθοδήγηση με σκοπό τη διασφάλιση συμμόρφωσης με τον GDPR και εξελίσσοντας την Γνωμοδότηση 15/2011 αναφορικά με τη συγκατάθεση.

Η συγκατάθεση παραμένει η μία από τις έξι νόμιμες βάσεις για την επεξεργασία προσωπικών δεδομένων, σύμφωνα με την κατηγοριοποίηση του άρθρου 6 του GDPR. Κατά την έναρξη δραστηριοτήτων που εμπεριέχουν επεξεργασία προσωπικών δεδομένων, ένας υπεύθυνος επεξεργασίας πρέπει πάντα να αφιερώνει χρόνο για να αξιολογήσει εάν η κατάλληλη νόμιμη βάση για την επικείμενη επεξεργασία είναι η συγκατάθεση ή εάν αντίθετα μία άλλη βάση πρέπει να επιλεγεί. Γενικά, η συγκατάθεση μπορεί να αποτελέσει κατάλληλη νόμιμη βάση εάν σε ένα υποκείμενο δεδομένων προσφέρεται έλεγχος και προσφέρεται μία γνήσια επιλογή αναφορικά με την αποδοχή ή απόρριψη των όρων που έχουν προσφερθεί ή απορριφθεί αυτών χωρίς ζημία. Όταν αιτείται συγκατάθεση, ένας ελεγκτής έχει καθήκον να αξιολογήσει κατά πόσο αυτό πληροί όλες τις απαιτήσεις για την απόκτηση έγκυρης συγκατάθεσης. Σε περίπτωση απόκτησης σε πλήρη συμμόρφωση με τον GDPR, η συγκατάθεση είναι ένα εργαλείο που δίνει στα υποκείμενα δεδομένων τον έλεγχο σχετικά με το κατά πόσο ή όχι τα προσωπικά δεδομένα που τους αφορούν θα υποστούν επεξεργασία. Σε αντίθετη περίπτωση, ο έλεγχος του υποκειμένου δεδομένων καθίσταται πλασματικός και η συγκατάθεση θα αποτελεί μία άκυρη βάση για επεξεργασία, καθιστώντας την δραστηριότητα επεξεργασίας παράνομη. Οι υπάρχουσες γνωμοδοτήσεις της Ομάδας Εργασίας του άρθρου 29 (WP29) σχετικά με τη συγκατάθεση παραμένουν σχετικές, όπου είναι συνεπείς με το νέο νομικό πλαίσιο, καθώς ο GDPR κωδικοποιεί την

υπάρχουσα καθοδήγηση και γενική καλή πρακτική της WP29 και τα περισσότερα από τα καθοριστικά στοιχεία της συγκατάθεσης παραμένουν τα ίδια υπό το καθεστώς του GDPR. Για το λόγο αυτό, σε αυτό το έγγραφο, η WP29 επεκτείνει και ολοκληρώνει προηγούμενες Γνωμοδοτήσεις σε συγκεκριμένα θέματα που περιλαμβάνουν αναφορά στη συγκατάθεση υπό το καθεστώς της οδηγίας 95/46/ΕΚ, χωρίς να τις αντικαθιστά.

Όπως αναφέρεται στην Γνωμοδότηση 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, η πρόσκληση σε άτομα για αποδοχή μίας πράξης επεξεργασίας δεδομένων θα πρέπει να υπόκειται σε αυστηρές απαιτήσεις, καθώς αφορά τα θεμελιώδη δικαιώματα των υποκειμένων δεδομένων και ο ελεγκτής δεν επιθυμεί να εμπλακεί σε μία πράξη επεξεργασίας που ενδέχεται να είναι παράνομη χωρίς τη συγκατάθεση του υποκειμένου επεξεργασίας. Ο κρίσιμος ρόλος της συγκατάθεσης υπογραμμίζεται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Επιπλέον, η απόκτηση συγκατάθεσης επίσης δεν αρνείται ή με οποιονδήποτε τρόπο δεν υποβαθμίζει τις υποχρεώσεις του ελεγκτή να τηρεί τις αρχές της επεξεργασίας που κατοχυρώνονται στον GDPR, ιδίως το άρθρο 5 του GDPR αναφορικά με την αντικειμενικότητα, την αναγκαιότητα και την αναλογικότητα, καθώς και με την ποιότητα των δεδομένων. Ακόμα και αν η επεξεργασία των προσωπικών δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου δεδομένων, αυτό δε νομιμοποιεί τη συλλογή δεδομένων η οποία δεν είναι αναγκαία σε σχέση με ένα συγκεκριμένο σκοπό επεξεργασίας και είναι θεμελιωδώς αθέμιτη. (Μήτρου , 2017)

Συνεπώς παρατηρούμε πως η επεξεργασία καθίσταται επιτρεπτή και νόμιμη όταν επίσης υπάρχει συγκατάθεση του υποκειμένου των δεδομένων. Ο νέος Κανονισμός διαφοροποιείται και σ’ αυτό το σημείο από το προηγούμενο νομικό καθεστώς, έτσι ώστε η συγκατάθεση του υποκειμένου να γίνεται με τρόπο σαφή, διακριτό από άλλα θέματα και απλά διατυπωμένο. Περαιτέρω το ίδιο υποκείμενο θα πρέπει να έχει ανά πάσα στιγμή το δικαίωμα της ανάκλησης της συγκατάθεσης. Έτσι λοιπόν, ο GDPR, επιβάλλει τη συμμόρφωση με τους κανονισμούς του τόσο των επιχειρήσεων όσο και των ατόμων που επεξεργάζονται στοιχεία. Υπό τους όρους του GDPR, όχι μόνο οι οργανισμοί θα πρέπει να εξασφαλίσουν ότι τα προσωπικά δεδομένα έχουν αποκτηθεί νόμιμα και υπό αυστηρές προϋποθέσεις, αλλά και αυτοί που συλλέγουν και διαχειρίζονται δεδομένα, θα είναι υποχρεωμένοι να τα

προστατεύουν από κατάχρηση και εκμετάλλευση, καθώς επίσης και να σέβονται τα δικαιώματα των υποκειμένων των δεδομένων. Σε διαφορετική περίπτωση, θα τους επιβάλλονται πρόστιμα και κυρώσεις.

3.4 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment - DPIA)

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων έχει στόχο την προστασία των φυσικών προσώπων και ειδικότερα των θεμελιωδών δικαιωμάτων και ελευθεριών τους, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας αυτών. Πιο συγκεκριμένα σύμφωνα με αυτά που ορίζονται στο Άρθρο 35, κάθε δημόσιος ή ιδιωτικός οργανισμός που επεξεργάζεται συγκεκριμένα προσωπικά δεδομένα, υποχρεούται πριν από την επεξεργασία να εκτελεί μια εκτίμηση των πιθανών επιπτώσεων των κινδύνων που μπορεί να προκύψουν από την επεξεργασία των δεδομένων αυτών.

Όπως ήδη αναφέρθηκε, ο Υπεύθυνος Επεξεργασίας και ο Εκτελών την Επεξεργασία υποχρεούνται σε τήρηση της αρχής της λογοδοσίας κατά την επεξεργασία δεδομένων, καθώς οι ενέργειές τους δεν αρκεί να είναι σύμφωνες με τα οριζόμενα στον Κανονισμό αλλά πρέπει και να είναι διαρκώς σε θέση να αποδείξουν ότι έχουν λάβει όλα τα ενδεδειγμένα μέτρα για τη συμμόρφωση αυτή. Η Εκτίμηση Αντικτύπου βοηθάει στην εκπλήρωση και των δύο πτυχών της αρχής της λογοδοσίας. Και αυτό γιατί, ανάλογα με τον κίνδυνο που μπορεί να προκύψει από την επεξεργασία των δεδομένων, όπως η στάθμιση του κινδύνου αυτού προέκυψε κατά την εκπόνηση της Εκτίμησης Αντικτύπου, προκύπτουν και τα μέτρα που θα κριθούν ως ενδεδειγμένα για την αντιμετώπισή του.

Σύμφωνα με τις κατευθυντήριες γραμμές της ομάδας του άρθρου 29, η εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων αποτελεί στην ουσία μια διαδικασία η οποία διενεργείται κυρίως κατά το αρχικό στάδιο σχεδίασης της εφαρμογής, και έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Αποτέλεσμα αυτής της διαδικασίας είναι η σύνταξη μιας έκθεσης στην οποία περιέχονται όλα τα στοιχεία και χαρακτηριστικά της επεξεργασίας, η εκτίμηση των πιθανών κινδύνων καθώς και προτεινόμενα μέτρα ασφαλείας ώστε να επιτυγχάνεται ο περιορισμός ή η εξάλειψη αυτών. Η έκθεση αυτή υπόκειται σε έλεγχο από την εκάστοτε Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ώστε να εκδώσει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων, όπως προβλέπεται από τον GDPR. Το γεγονός ότι εκτελείται κατά το αρχικό στάδιο σχεδίασης της εφαρμογής δίνει το πλεονέκτημα της πρόληψης και της αντιμετώπισης των κινδύνων, όπως επίσης και της αποφυγής οικονομικής ζημιάς για τον οργανισμό, σε περίπτωση που οι επιπτώσεις των κινδύνων επεκταθούν σε κάποιον από τους εμπλεκόμενους στην επεξεργασία. (Σιασιάκος , Αναστασίου , & Τούντας , 2016)

Η εκτίμηση αυτή είναι απαραίτητη κάθε φορά που η επεξεργασία ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σύμφωνα με τον Κανονισμό, η εκπόνηση της απαιτείται α) όταν πραγματοποιείται συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών ενός φυσικού προσώπου, συμπεριλαμβανομένης της κατάρτισης προφίλ, β) όταν πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή γ) όταν παρακολουθούνται συστηματικά δημόσια προσπελάσιμοι χώροι σε μεγάλη κλίμακα.

Όπως γίνεται αντιληπτό, η επιτυχία της Εκτίμησης Αντικτύπου συνδέεται ευθέως με το χρονικό σημείο στο οποίο αυτή θα διεξαχθεί. Όσο νωρίτερα εντοπιστούν κατά το σχεδιασμό ενός νέου έργου, συστήματος ή μιας οποιασδήποτε νέας διαδικασίας, ευρήματα που μπορεί να οδηγούν σε «κίνδυνο» για τα προσωπικά δεδομένα, τόσο μεγαλύτερη θα είναι η ακρίβεια και η αποτελεσματικότητα των μέτρων που θα ληφθούν και θα ενσωματωθούν για την προστασία των δεδομένων αυτών. Η διαδικασία έγκαιρης διάγνωσης, εντοπισμού των πιθανών κινδύνων και ενσωμάτωσης των κατάλληλων μέτρων προστασίας κατά το σχεδιασμό είναι γνωστή ως “privacy by design”. Παράλληλα με την έγκαιρη εκπόνησή της, παράγοντα επιτυχίας της Εκτίμησης Αντικτύπου θα αποτελέσει και η εμπλοκή των κατάλληλων ανθρώπων, εκείνων με την κατάλληλη εμπειρία και γνώση και, σε κάθε περίπτωση, του DPO. Έτσι, η DPIA πρέπει να θεωρείται ένα κομμάτι από μια ευρύτερη διαδικασία διαχείρισης κινδύνων (risk management) που οφείλει να εφαρμόζει ένας οργανισμός. Παρ’ όλο που ονομάζεται εκτίμηση ή αξιολόγηση, η DPIA δεν είναι μια απλή ανάλυση κινδύνων αλλά περιλαμβάνει όλα τα απαραίτητα μέτρα ασφαλείας ή

ελέγχου σε σχέση με τους πιθανούς κινδύνους (Κοτσαλής & Μενουδάκος , 2018). Σε κάθε περίπτωση, αφορμή για σκέψη πάνω σε θέματα στάθμισης κόστους- κινδύνου μπορεί να δώσει η διαπίστωση του Richard Clarke, ειδικού συμβούλου σε θέματα κυβερνοασφάλειας του τέως Προέδρου των Ηνωμένων Πολιτειών Ronald Reagan: «Εάν ξοδεύεις περισσότερα χρήματα για καφέ παρά για ασφάλεια πληροφοριακών συστημάτων, θα πέσεις θύμα κακόβουλης επίθεσης. Επιπλέον, θα το αξίζεις». (Ομάδα εργασίας του ΣΕΒ για τα προσωπικά δεδομένα, Οκτώβριος 2018)

3.4.1 Επιπτώσεις από την εφαρμογή του GDPR στις ελληνικές επιχειρήσεις

Οι ελληνικές επιχειρήσεις, ανάλογα με το μέγεθος τους κάθε φορά, παρουσιάζουν μία γενικά θετική εικόνα στην ψηφιακή τους προστασία. Αυτό όμως που λείπει, είναι η εταιρική κουλτούρα, γιατί «ψηφιακή προστασία» δεν σημαίνει μόνο ασφάλεια των συστημάτων αλλά και προστασία των προσωπικών δεδομένων.

Οι ίδιες οι οικονομικές οντότητες, θα πρέπει πρώτα να κατανοήσουν την σπουδαιότητα και την αξία των δεδομένων που έχουν στην διάθεσή τους, καθώς και γιατί οι πολιτικές που ακολουθούνται – από τα ανεξαρτήτως βαθμίδας στελέχη τους – θα πρέπει να συντείνουν σε αυτό το σκοπό, και να επενδύσουν και τυπικά και ουσιαστικά στην υλοποίησή τους. Αν τα κράτη μέλη της ΕΕ θέλουν να είναι όντως ευνομούμενα σε όλες τις εκφάνσεις της διοίκησης τους, πρέπει να θεσπίσουν τα αναγκαία μέτρα και μηχανισμούς. Η τεχνολογική εξέλιξη δεν μπορεί από μόνη της να παράσχει αυτή την προστασία. Άλλωστε, το κάθε τεχνολογικό επίτευγμα εξ ορισμού μπορεί ανά πάσα στιγμή να είναι «παρωχημένο». Η γνώση, η ευαισθητοποίηση και η λογοδοσία πρέπει να γίνουν ο ακρογωνιαίος λίθος για κάθε επιχείρηση που θέλει να προστατεύσει τα προσωπικά δεδομένα, τα οποία αποτελούν το σημαντικότερο περιουσιακό της στοιχείο.

Πολλές από τις μεγάλες ελληνικές επιχειρήσεις και οργανισμούς ασχολούνται με το θέμα της συμμόρφωσης, αλλά πρακτικά ελάχιστες είναι εκείνες που έχουν ολοκληρώσει το συγκεκριμένο έργο, το οποίο απαιτεί συντονισμό μίας μεγάλης ομάδας στελεχών και διαμόρφωση εξειδικευμένων διαδικασιών.

Ωστόσο, στο ζήτημα του GDPR που θα πρέπει να επισημανθεί είναι ότι η Ελλάδα δεν βρίσκεται πίσω από τις υπόλοιπες χώρες της ΕΕ, καθώς και εκεί παρουσιάζονται αρκετές καθυστερήσεις.

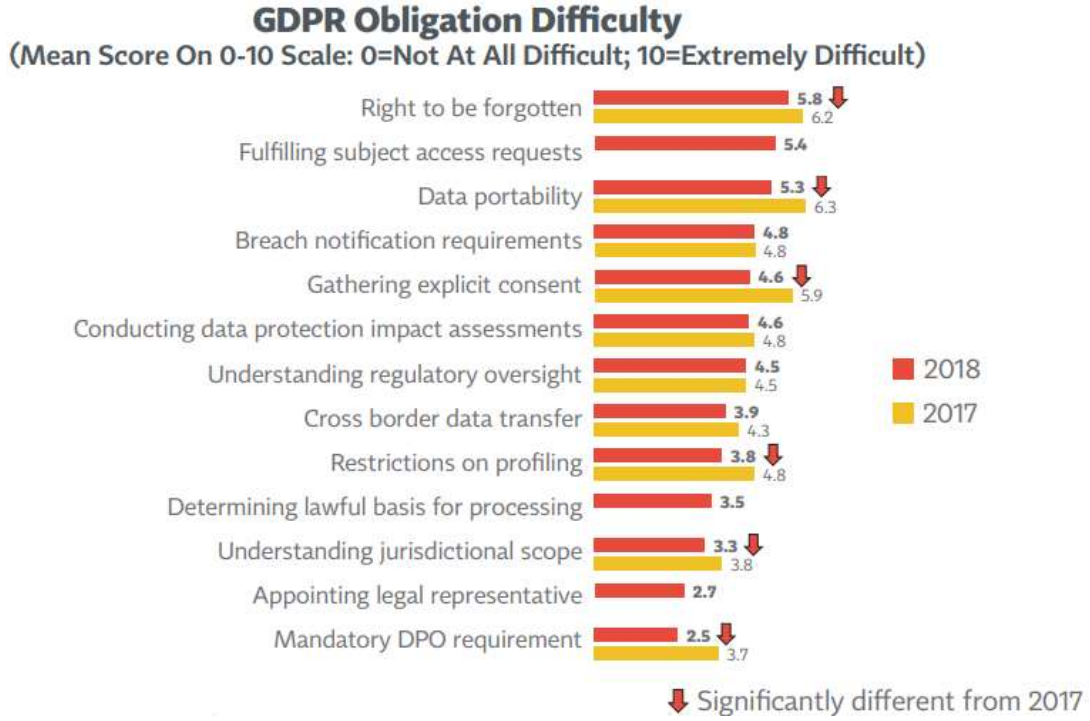
Κάθε ελληνική επιχείρηση που διατηρεί σε υπολογιστή δεδομένα πρέπει να συντάξει έκθεση διαχείρισης αυτών και να συμβουλευτεί την αρμόδια Αρχή για το εάν θα πρέπει να συμμορφωθεί με το νέο Κανονισμό. Εάν είναι υπόχρεη, θα πρέπει να ορίσει έναν υπεύθυνο διαχείρισης και προστασίας δεδομένων ο οποίος δεν μπορεί να είναι ο τεχνικός Ηλεκτρονικών Υπολογιστών - Δικτύων, δηλαδή ο επικεφαλής του υπάρχοντος Πληροφοριακού Συστήματος, λόγω σύγκρουσης συμφερόντων.

Ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer - DPO) θα είναι το «δεξί χέρι» του μάνατζερ και θα πρέπει να συγκροτήσει ομάδα ειδικών και με νομική συμβολή ώστε να απεξαρτηθεί από την πληροφόρηση που προέρχεται από μονάδες και πρόσωπα που μπορεί να προστατεύουν ξεπερασμένα και επικίνδυνα για διαρροές πληροφοριακά συστήματα.

Στη συνέχεια, η εταιρεία πρέπει να εξετάσει την αλλαγή ή και προσαρμογή των πληροφοριακών της συστημάτων για να συμμορφωθεί με τους όρους που θέτει ο Κανονισμός. Συνοπτικά, τα σημεία που πρέπει να προσέξουν οι επιχειρήσεις κατά την εφαρμογή του Κανονισμού, είναι:

- Διαχείριση του κόστους που επιβαρύνει την καθημερινή λειτουργία για την επίτευξη συμμόρφωσης
- Επιλογή των κατάλληλων στελεχών ή / και εξωτερικών συνεργατών (κύριο κριτήριο επιλογής: αξιοπιστία και αποτελεσματικότητα)
- Λανθασμένη εντύπωση ότι δεν εμπίπτουν στον Κανονισμό και ως εκ τούτου ότι δεν χρειάζεται να προβούν σε καμία δράση συμμόρφωσης.
- Λανθασμένη εντύπωση ότι δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους και ότι είναι ασφαλείς
- Σημεία υψηλής τεχνικότητας:
- Φορητότητα των δεδομένων
- Δικαίωμα στη λήθη
- Εξασφάλιση συγκατάθεσης υποκειμένου

- ❖ Συμβάσεις με τρίτα μέρη - Σχέσεις με Εκτελούντες την Επεξεργασία (Ομάδα εργασίας του ΣΕΒ για τα προσωπικά δεδομένα, Οκτώβριος 2018)



Εικόνα2: Σημεία συμμόρφωσης στον Κανονισμό που δυσκολεύουν τις επιχειρήσεις, 2017-2018. (Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017)

3.4.2 Επιπτώσεις από την επιβολή του GDPR στον Δημόσιο Τομέα

Όσον αφορά την εφαρμογή του GDPR στον Δημόσιο Τομέα, το Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, μέσω της αρμόδια Γενικής Γραμματείας Ψηφιακής Πολιτικής, συνεργάστηκε με τα αρμόδια Υπουργεία και τις Ανεξάρτητες Ρυθμιστικές Αρχές για την άμεση ενσωμάτωση του νέου Κανονισμού.

Στόχος αποτελεί ο σχεδιασμός ενός ολοκληρωμένου σχεδίου ασφαλείας και η ανάπτυξη ενιαίας πλατφόρμας που θα υιοθετεί τα απαιτούμενα τεχνικά, διαδικαστικά και οργανωτικά μέτρα που απαιτούνται για την προστασία των πληροφοριακών συστημάτων. Η Γενική Γραμματεία θα συντονίσει μεγάλους φορείς, όπως η ΗΔΙΚΑ (Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης), η ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων), ο ΕΟΠΥΥ (Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας) και το ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας), οι

οποίοι κατέχουν μεγάλο όγκο προσωπικών δεδομένων, ώστε να εναρμονιστούν με τον Κανονισμό GDPR για την προστασία των προσωπικών δεδομένων.

Επιπλέον, η Γενική Γραμματεία συμμετέχει στην ομάδα εναρμόνισης της Εθνικής νομοθεσίας με την οδηγία NIS (Network and Information Security), αλλά και στο cooperation group, όπου γίνεται ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών.

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.

Μέχρι στιγμής, 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. Το προαναφερθέν έχει μείνει ακόμη στα χαρτιά και δεν έχουν πραγματοποιηθεί ακόμη οι απαραίτητες ενέργειες συμμόρφωσης με τον GDPR στο δημόσιο τομέα.

3.5 Πρόστιμα και κυρώσεις

Η Ευρωπαϊκή Ένωση έχει ολοκληρώσει μια εκτεταμένη μεταρρύθμιση του νομοθετικού πλαισίου για την προστασία των δεδομένων στην Ευρώπη, βασιζόμενη σε συγκεκριμένους άξονες. Η συνεπής εφαρμογή των κανόνων προστασίας των δεδομένων αποτελεί κεντρικό στοιχείο ενός εναρμονισμένου καθεστώτος προστασίας δεδομένων.

Τα διοικητικά πρόστιμα αποτελούν κεντρικό στοιχείο του νέου καθεστώτος επιβολής που έχει θεσπιστεί με τον GDPR, και είναι ένα ισχυρό εργαλείο στα χέρια των εποπτικών αρχών, μαζί με τα άλλα μέτρα που προβλέπονται στο άρθρο 58, για την εφαρμογή των νέων διατάξεων. Στο πλαίσιο αυτό, η Ομάδα Εργασίας του Άρθρου 29 δημοσίευσε ένα νέο έγγραφο με κατευθυντήριες γραμμές για την εφαρμογή των διατάξεων του GDPR σχετικά με την επιβολή διοικητικών προστίμων.

Συγκεκριμένα, σύμφωνα με το άρθρο 70, παρ. 1, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) έχει την εξουσία να εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές, προκειμένου να διασφαλίσει τη συνεκτική εφαρμογή του παρόντος κανονισμού. Επιπρόσθετα, σύμφωνα με το ίδιο άρθρο, το EDPB εκπονεί κατευθυντήριες γραμμές για τις εποπτικές αρχές όσον αφορά την εφαρμογή των μέτρων που αναφέρονται στο άρθρο 58 παράγραφοι 1, 2 και 3 και τον καθορισμό διοικητικών προστίμων δυνάμει του άρθρου 83.

Προκειμένου να επιτευχθεί μια συνεκτική προσέγγιση στην επιβολή των διοικητικών προστίμων, το EDPB συμφώνησε σε μια κοινή κατανόηση των κριτηρίων αξιολόγησης του άρθρου 83 παρ. 2 του Κανονισμού και επομένως το EDPB και οι εθνικές εποπτικές αρχές συμφωνούν να χρησιμοποιήσουν τις κατευθυντήριες γραμμές ως κοινό έδαφος για μία ενιαία προσέγγιση.

Σύμφωνα λοιπόν με τις διατάξεις του GDPR, η μη συμμόρφωση με τον Κανονισμό μπορεί να οδηγήσει τις εποπτικές αρχές στην επιβολή διοικητικού προστίμου που κυμαίνεται από 20 εκατομμύρια ευρώ έως 4% του παγκόσμιου ετήσιου κύκλου εργασιών της εταιρείας του προηγούμενου οικονομικού έτους, ποσό το οποίο για κάποιους θα μπορούσε να σημαίνει δισεκατομμύρια. Τα πρόστιμα θα εξαρτηθούν από τη σοβαρότητα της παραβίασης και από το εάν η εταιρεία θεωρείται ότι έλαβε σοβαρά υπόψιν της τα εφαρμοστέα μέτρα και τους κανόνες σχετικά με την ασφάλεια. (Voigt & Bussche , 2017)

Η έλλειψη συμμόρφωσης μπορεί να συνεπάγεται:

- Ελέγχους και επιβολή κυρώσεων από την Αρχή (συστάσεις, πρόστιμα, απαγορεύσεις, ανακλήσεις αδειών).
- 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

Ένα μικρότερο πρόστιμο ύψους 10 εκατομμυρίων ευρώ ή 2% του παγκόσμιου κύκλου εργασιών θα εφαρμοστεί σε εταιρείες που κακοδιαχειρίζονται δεδομένα με άλλους τρόπους. Περιλαμβάνουν, μεταξύ άλλων, την αδυναμία δήλωσης παραβίασης

των δεδομένων, την αδυναμία οικοδόμησης της προστασίας της ιδιωτικής ζωής από το σχεδιασμό, την εξασφάλιση της προστασίας των δεδομένων κατά το πρώτο στάδιο ενός έργου και την αδυναμία συμμόρφωσης ως προς τον διορισμό ενός Υπευθύνου Προστασίας Δεδομένων.

Εικόνα 3: Ενέργειες προς αποφυγή για την μη επιβολή προστίμων. Πηγή: https://gdprcoalition.ie

Για την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη, μεταξύ άλλων τα ακόλουθα:

I. Η φύση, η βαρύτητα και η διάρκεια της παράβασης, καθώς και ο αριθμός των υποκειμένων που έθιξε η παράβαση και ο βαθμός ζημίας που υπέστησαν.

II. Ο δόλος ή η αμέλεια που προκάλεσε την παράβαση.

III. Οποιεσδήποτε, ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων.

IV. Ο βαθμός ευθύνης του υπεύθυνου επεξεργασίας, λαμβάνοντας υπόψη τα μέτρα που εφάρμοσε.

V. Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των επιπτώσεών της.

VI. Οι κατηγορίες προσωπικών δεδομένων που επηρέασε η παράβαση.

VII. Η τήρηση εγκεκριμένων κωδικών δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης.

Ο Κανονισμός αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να υποβάλουν καταγγελία στην εποπτική αρχή καθώς και το δικαίωμά τους για λήψη δικαστικών μέτρων και απαίτηση αποζημιώσεως. Συνεπώς παραβιάσεις όπως πρόσβαση στον εξυπηρετητή από hackers, κλοπή εγγράφων, καταστροφή πρωτοτύπων, απλή διαρροή δεδομένων μισθοδοσίας ή ονομάτων, όπως για παράδειγμα η πρόσφατη καταγγελία για διαρροή τηλεπικοινωνιακών στοιχείων πελατών από υπάλληλο οργανισμού του ευρύτερου δημόσιου τομέα, αλλά και συλλογή αρχείου τρίτων προσώπων άνευ συναίνεσης άλλης βάσης επεξεργασίας, δύνανται να προκαλέσουν αξιώσεις σοβαρών αποζημιώσεων.

Ασφαλώς, επιχειρήσεις οι οποίες ευθύνονται για μικρές παραβιάσεις του Κανονισμού δεν πρέπει να ανησυχούν για την επιβολή των αυστηρότερων κυρώσεων αλλά ούτε και να τρομοκρατηθούν εξαιτίας των εξαντλητικών κυρώσεων και να θεωρήσουν ότι η εφαρμογή του Κανονισμού αποτελεί την μεγαλύτερη απειλή για τις επιχειρήσεις. Από την άλλη μεριά όμως, αποτελεί παραδεκτό γεγονός ότι ο GDPR παρέχει την εξουσία στις αρχές να επιβάλλουν υψηλά έως και εξοντωτικά πρόστιμα αλλά και μια σειρά άλλων εργαλείων για τον έλεγχο συμμόρφωσης και εφαρμογής του Κανονισμού. (Μήτρου , 2017)

3.6 Πρόσθετες επιπτώσεις για τα φυσικά πρόσωπα από τον GDPR

Η ραγδαία τεχνολογική εξέλιξη στον τομέα της πληροφορικής και η βίαιη εισβολή στις ζωές όλων μας των υπολογιστών, tablet καθώς και του Internet, έχει οδηγήσει τους πολίτες όλων των κρατών σε αλλαγή του τρόπου ζωής τους και σε άμεση εξάρτηση από τέτοιου είδους τεχνολογικά μέσα. Το Internet έχει εισβάλει για τα καλά στις ζωές μας, ενώ η εφεύρεση ιστοσελίδων κοινωνικής δικτύωσης, έχει καταστήσει τα προσωπικά μας δεδομένα ευάλωτα στον κάθε επιτήδειο.

Δεν είναι λίγες οι φορές που αρκετοί μας συνάνθρωποι διάσημοι ή μη έχουν πέσει θύμα παραβιάσεων και εκμετάλλευσης των δεδομένων τους, είτε πρόκειται για στοιχεία ηλεκτρονικού ταχυδρομείου, είτε για κωδικό πρόσβασης, αριθμό κοινωνικής ασφάλισης, ή για εμπιστευτικά προσωπικά αρχεία.

Μια από τις σημαντικότερες αλλαγές που έχει φέρει ο GDPR είναι η παροχή στους καταναλωτές του δικαιώματος να γνωρίζουν πότε έχουν αλλοιωθεί τα

δεδομένα τους. Οι οντότητες θα πρέπει να ενημερώσουν το συντομότερο δυνατόν τους αρμόδιους εθνικούς φορείς, προκειμένου να διασφαλίσουν ότι οι πολίτες μπορούν να λάβουν τα κατάλληλα μέτρα για να αποτρέψουν την κατάχρηση των δεδομένων τους.

Εξασφαλίζεται, επίσης ευκολότερη πρόσβαση στα δεδομένα των καταναλωτών ως προς τον τρόπο που αναλύονται και επεξεργάζονται, με τους οργανισμούς να ισχυρίζονται ότι πρέπει να αναλύσουν λεπτομερώς τον τρόπο με τον οποίο χρησιμοποιούν τις πληροφορίες των πελατών με τρόπο σαφή και κατανοητό.

Οι περισσότερες επιχειρήσεις, διαδικτυακά e-shop έχουν ήδη αποστείλει μηνύματα ηλεκτρονικού ταχυδρομείου στους πελάτες τους με πληροφορίες σχετικά με τον τρόπο χρήσης των δεδομένων τους. Πολλοί οργανισμοί, όπως αυτοί στους κλάδους λιανικής και μάρκετινγκ, έρχονται σε επαφή με πελάτες για να ρωτήσουν αν θέλουν να είναι μέρος της βάσης δεδομένων τους. Υπό αυτές τις συνθήκες, ο πελάτης θα πρέπει να έχει έναν εύκολο τρόπο να αποχωρήσει από τα στοιχεία του που βρίσκονται σε μια λίστα αλληλογραφίας.

Ο νέος Κανονισμός, φέρνει μεταξύ άλλων ένα σύνολο αλλαγών, μεταρρυθμίσεων και νέων ενισχυμένων δικαιωμάτων για τους πολίτες των κρατών-μελών της Ευρωπαϊκής Ένωσης. Τα υποκείμενα των δεδομένων αποκτούν μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, αφού έχουν πλέον:

α) Δικαίωμα πρόσβασης του υποκειμένου στα δεδομένα που τηρούνται σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ

β) Δικαίωμα εναντίωσης του υποκειμένου στην ανωτέρω επεξεργασία, ιδίως για σκοπούς απευθείας εμπορικής προώθησης

γ) Δικαίωμα διαγραφής (δικαίωμα στη λήθη), κατά το οποίο, το υποκείμενο των δεδομένων διατηρεί το δικαίωμα να αιτηθεί στον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση, γεγονός στο οποίο ο υπεύθυνος επεξεργασίας υποχρεούται να πειθαρχήσει χωρίς αδικαιολόγητη καθυστέρηση, εφόσον ισχύει ένας από τους προβλεπόμενους στον Κανονισμό λόγους. Έτσι, λοιπόν όταν ένα άτομο δεν επιθυμεί πλέον την επεξεργασία των δεδομένων του και δεν υπάρχει νόμιμος λόγος για να τη διατήρησή τους, τα δεδομένα θα διαγράφονται. Το δικαίωμα διαγραφής συνηθίζεται

να αποκαλείται και ως δικαίωμα στη λήθη, χωρίς όμως ο όρος αυτός να είναι απολύτως ακριβής, διότι η λήθη στο διαδίκτυο δεν είναι απολύτως εφικτή .

δ) Δικαίωμα φορητότητας των δεδομένων: το υποκείμενο των δεδομένων δικαιούται να λαμβάνει τα δεδομένα που το αφορούν, ενώ τα είχε παράσχει σε υπεύθυνο επεξεργασίας σε μορφή δομημένη, κοινώς χρησιμοποιούμενη και αναγνωρίσιμη από μηχανήματα και να τα διαβιβάζει σε άλλο υπεύθυνο επεξεργασίας. Συνεπώς, καθίσταται ευκολότερη η διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ παρόχων υπηρεσιών.

ε) Υποχρέωση ενημέρωσης σε περίπτωση παραβιάσεων: Οι υπεύθυνοι επεξεργασίας, έχουν υποχρέωση, εκτός του να παρέχουν «διαφανείς» και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων, να ενημερώσουν τις αρμόδιες Αρχές, μόλις αντιληφθούν παραβίαση, αλλά και τα ίδια τα φυσικά πρόσωπα, των οποίων παραβιάστηκαν τα δεδομένα, εφ' όσον η παραβίαση τα θέτει σε σοβαρό κίνδυνο.

στ) Προστασία δεδομένων κατά το σχεδιασμό («Data protection by design»): Επιβάλλεται η δημιουργία προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων τους.

ζ) Προστασία δεδομένων εξ' ορισμού («Data protection by default»): Επιβάλλεται η εφαρμογή κατάλληλων μέτρων που θα διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας.

η) Ειδική πρόβλεψη για την προστασία δεδομένων των παιδιών

Ωστόσο, και τα ίδια τα υποκείμενα των δεδομένων δεν θα πρέπει να ξεχνάνε ότι η ιδιωτική τους ζωή είναι πολύτιμη. Οι ίδιοι οι πολίτες έχουν τον πρώτο και τον τελευταίο λόγο στο να επιλέγουν ποιες πληροφορίες δίνουν στους άλλους και ποιες διατηρούν μόνο για τον εαυτό τους. Εκείνοι και μόνο εκείνοι είναι υπεύθυνοι να διατηρούν τον έλεγχο των προσωπικών τους δεδομένων και της ιδιωτικής τους ζωής. Συνεπώς, πρέπει πάντα να σκεφτόμαστε πριν δημοσιεύσουμε κάτι στο διαδίκτυο ή πριν δώσουμε πληροφορίες προσωπικών μας δεδομένων σε τρίτους. (Voigt & Bussche , 2017)

3.6.1 Το GDPR για τα παιδιά

Σε σύγκριση με την παλαιά οδηγία, το GDPR δημιουργεί ένα πρόσθετο επίπεδο προστασίας, το οποίο αφορά τα προσωπικά δεδομένα ευάλωτων φυσικών προσώπων, όπως είναι τα παιδιά. Σύμφωνα με το άρθρο 8 παρ. 1 του νέου Κανονισμού, η διάθεση ψηφιακών υπηρεσιών σε παιδιά κάτω των 18 ετών θα επιτρέπεται μόνο αν το παιδί είναι τουλάχιστον 16 ετών, ενώ για παιδιά ηλικίας από 13-16 ετών θα απαιτείται η συναίνεση του γονέα ή κηδεμόνα. Ο νέος κοινός ευρωπαϊκός νόμος δίνει το περιθώριο σε κάθε χώρα-μέλος να νομοθετήσει για ελεύθερη πρόσβαση στο διαδίκτυο παιδιών μικρότερης ηλικίας με κατώτατο επιτρεπόμενο όριο τα 13 έτη. Ήδη κάποιες από τις χώρες-μέλη έχουν πάρει τις οριστικές αποφάσεις για το θέμα και πολύ σύντομα θα διευκρινιστεί και το τοπίο στην Ελλάδα, αφού ληφθούν υπόψη οι εισηγήσεις όλων των εμπλεκόμενων φορέων και αρχών.

Επιπλέον, ο νέος Κανονισμός ορίζει την ευθύνη του Υπευθύνου Επεξεργασίας, ο οποίος οφείλει να καταβάλλει κάθε δυνατή προσπάθεια, προκειμένου να εξακριβώσει την ηλικία του υποκειμένου των δεδομένων, ειδικά όταν πρόκειται για παιδιά. Ειδικότερα, πρέπει να σημειωθεί ότι ένας υπεύθυνος επεξεργασίας που παρέχει διασυνοριακή υπηρεσία δεν μπορεί πάντα να βασίζεται στη συμμόρφωση μόνο με το δίκαιο του κράτους μέλους στο οποίο έχει την κύρια εγκατάστασή του, αλλά μπορεί να χρειαστεί να συμμορφωθεί με τις αντίστοιχες εθνικές νομοθεσίες κάθε κράτους μέλους που προσφέρει η υπηρεσία ή οι κοινωνικές υπηρεσίες.

Κατά την παροχή κοινωνικών υπηρεσιών στα παιδιά με βάση τη συγκατάθεσή τους, οι υπεύθυνοι επεξεργασίας θα πρέπει να καταβάλουν λογικές προσπάθειες για να επαληθεύσουν ότι ο χρήστης υπερβαίνει την ηλικία της ψηφιακής συγκατάθεσης και ότι τα μέτρα αυτά πρέπει να είναι ανάλογα με τη φύση και τους κινδύνους των δραστηριοτήτων επεξεργασίας. Αυτό εξαρτάται από το εάν ένα κράτος μέλος επιλέγει να χρησιμοποιήσει τον τόπο της κύριας εγκατάστασης του υπεύθυνου επεξεργασίας ως σημείο αναφοράς στο εθνικό του δίκαιο ή την κατοικία του υποκειμένου των δεδομένων.

Εάν οι χρήστες δηλώσουν ότι είναι άνω της ηλικίας της ψηφιακής συγκατάθεσης τότε ο ελεγκτής μπορεί να πραγματοποιήσει τους κατάλληλους

ελέγχους για να βεβαιώσει ότι αυτή η δήλωση είναι αληθής. Παρόλο που η ανάγκη επαλήθευσης της ηλικίας δεν είναι ρητή στο GDPR, απαιτείται σιωπηρά, διότι εάν ένα παιδί δώσει συγκατάθεση ενώ δεν είναι αρκετά μεγάλο για να παράσχει έγκυρη συναίνεση για λογαριασμό του, τότε αυτό θα καταστήσει παράνομη την επεξεργασία των δεδομένων.

Εάν ο χρήστης δηλώσει ότι είναι κάτω από την ηλικία της ψηφιακής συγκατάθεσης τότε ο υπεύθυνος επεξεργασίας μπορεί να αποδεχθεί τη δήλωση αυτή χωρίς περαιτέρω ελέγχους αλλά θα πρέπει να συνεχίσει να λαμβάνει γονική άδεια και να επαληθεύσει ότι το πρόσωπο που παρέχει αυτή τη συγκατάθεση είναι κάτοχος γονικής μέριμνας .

Η επαλήθευση ηλικίας δεν πρέπει να οδηγήσει σε υπερβολική επεξεργασία δεδομένων. Ο μηχανισμός που επιλέγεται για την επαλήθευση της ηλικίας του υποκειμένου των δεδομένων πρέπει να περιλαμβάνει αξιολόγηση του κινδύνου της προτεινόμενης επεξεργασίας. Σε ορισμένες περιπτώσεις χαμηλού κινδύνου, μπορεί να είναι σκόπιμο να απαιτηθεί από έναν νέο συνδρομητή σε μια υπηρεσία να αποκαλύψει το έτος γέννησής του ή να συμπληρώσει ένα έντυπο που δηλώνει ότι είναι (ή όχι) ανήλικος. Εάν προκύψουν αμφιβολίες, ο ελεγκτής θα πρέπει να επανεξετάσει την ηλικία του μέσω μηχανισμού επαλήθευσης σε μια συγκεκριμένη περίπτωση και να εξετάσει εάν απαιτούνται εναλλακτικοί έλεγχοι. (Κοτσαλής & Μενουδάκος , 2018)

Ωστόσο, ένα θέμα που έχει απασχολήσει ιδιαίτερα τις αρχές της Ελλάδας, είναι η συμμετοχή των παιδιών στις νέες τεχνολογίες και το κατά πόσο είναι εφικτό, επιθυμητό και πρέπον να αφαιρεθεί στα παιδιά το δικαίωμα να συμμετέχουν ελεύθερα στις νέες τεχνολογίες και στις ευκαιρίες που προσφέρει ο ψηφιακός κόσμος.

Ο εκπρόσωπος της Αρχής Προστασίας Προσωπικών Δεδομένων επεσήμανε την αναγκαιότητα συνολικής ενισχυμένης προστασίας προσωπικών δεδομένων, ανεξαρτήτου ηλικίας του χρήστη του διαδικτύου, καθώς δεν είναι λίγοι οι ενήλικοι διαδικτυακός «αναλφάβητοι» που με πλήρη άγνοια κινδύνου εισέρχονται στο διαδίκτυο. Υπογράμμισε επίσης, την ευθύνη των παρόχων να αναζητήσουν και να εφαρμόσουν αποτελεσματικούς τρόπους ελέγχου της ηλικίας των παιδιών που κάνουν χρήση των κοινωνικών δικτύων έτσι ώστε να διασφαλίζεται το επιτρεπόμενο ηλικιακό όριο, που προς το παρόν τουλάχιστον, είναι τα 13 έτη. Ιδιαίτερη έμφαση

τέλος, δόθηκε και στην αλλαγή της μορφής των όρων χρήσης της κάθε εφαρμογής που στην παρούσα φάση χαρακτηρίζονται ατέρμονοι και δυσνόητοι με συνέπεια ο χρήστης να μην κατανοεί σε τι συναινεί. Συνεπώς, είναι επιτακτική ανάγκη η ενημέρωση των παιδιών αλλά και των κηδεμόνων τους, να γίνεται σε γλώσσα απλή και σαφή .

3.7 Πρόσθετες επιπτώσεις για τις επιχειρήσεις από την επιβολή του GDPR (άμεσα-έμμεσα κόστη)

Οι περισσότερες επιχειρήσεις ανησυχούν σχετικά με την εφαρμογή του νέου Κανονισμού, αλλά στην πραγματικότητα αυτό δεν χρειάζεται, διότι ναι μεν καθίστανται αυστηρότεροι κανόνες και μεγαλύτερες ποινές, αλλά οι βασικές αρχές της προστασίας των δεδομένων, παραμένουν ίδιες. Ο GDPR ουσιαστικά, αφορά περισσότερο τους τρόπους και τις διαδικασίες ελέγχου ως προς τη συμμόρφωση στη νομοθεσία, παρά δημιουργεί κάτι εντελώς νέο εξαρχής.

Το ζήτημα του επανασχεδιασμού των πληροφοριακών συστημάτων σαφώς προκαλεί τεράστιο κόστος, ενώ ο GDPR βάζει σε δοκιμασία και στρατηγικές συνεργασίες μεταξύ εταιρειών οι οποίες θα πρέπει να συμμορφωθούν ταυτόχρονα και με την ίδια αυστηρότητα στο νέο Κανονισμό προστασίας δεδομένων.

Για παράδειγμα, η συλλογή, η αποθήκευση και η διαχείριση των δεδομένων θα πρέπει να έχει ενταχθεί στο πληροφοριακό σύστημα της κάθε επιχείρησης από τον σχεδιασμό του ώστε να τηρούνται τα όρια. Ταυτόχρονα, οι προμηθευτές ή οι πελάτες χοντρικής που έχουν υιοθετήσει το νέο Κανονισμό, θα έχουν φραγμούς στη συσχέτιση βάσεων δεδομένων που θα μπορούσαν να οδηγήσουν σε αναγνώριση του πελάτη με πλήρη στοιχεία.

Αυτό δυνητικά δημιουργεί μια προβληματική συνθήκη για την εξατομίκευση των υπηρεσιών και τη στοχευμένη εμπορική πολιτική που αποσκοπεί στην ικανοποίηση του πελάτη. Όλες οι εταιρείες άλλωστε, αναπτύσσουν ειδικές πολιτικές πώλησης και προνομίων για τους «καλούς» πελάτες τους, ενώ οι διαφημιστικές μέσω του «profiling» επιτυγχάνουν να φτάνει το σωστό μήνυμα στον σωστό παραλήπτη.

Με την υιοθέτηση του GDPR, τα σημαντικότερα στοιχεία που υφίστανται τροποποιήσεις είναι :

1) Μεγαλύτερο προβάδισμα και εξουσία στα άτομα. Ο νέος Κανονισμός, τοποθετεί τα υποκείμενα των δεδομένων στο κέντρο της προστασίας των δεδομένων. Για παράδειγμα, το δικαίωμα στη φορητότητα των δεδομένων προβλέπει ότι όταν οι πελάτες θέλουν να αλλάξουν πάροχο για τα e-mail τους, θα πρέπει να μπορούν να μεταφέρουν το σύνολο των δεδομένων τους στο νέο πάροχο. Οι καταναλωτές μέχρι και πριν την ισχύ του Κανονισμού είχαν ήδη τη δυνατότητα να ζητήσουν την διαγραφή των προσωπικών τους στοιχείων, αλλά ο GDPR ενίσχυσε αυτό το δικαίωμα διαγραφής με το λεγόμενο **«δικαίωμα στη λήθη».** (Μήτρου , 2017) Ωστόσο, πέρα από τη συμμόρφωση, η μεγαλύτερη αλλαγή είναι η μετατόπιση της στάσης του οργανισμού απέναντι στην προστασία της ιδιωτικής ζωής. Η προστασία της ιδιωτικής ζωής τείνει να γίνει αντικείμενο σεβασμού για τις επιχειρήσεις. Στοιχείο-κλειδί θα είναι το να καταφέρουν να κερδίσουν την εμπιστοσύνη των πελατών και να αποκτήσουν ανταγωνιστικό πλεονέκτημα, ακριβώς επειδή οι πελάτες δίνουν μεγάλη αξία στην προστασία της ιδιωτικής τους ζωής.

2) Προστασία της ιδιωτικότητας ήδη από το στάδιο του σχεδιασμού. Το πρώτο βήμα για κάθε οργανισμό θα είναι μια άσκηση χαρτογράφησης της ροής των δεδομένων στην οποία θα συμμετέχει το σύνολο του οργανισμού, επειδή η προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό προϋποθέτει ότι όλες οι υπηρεσίες θα εξετάσουν τα δεδομένα τους και τον τρόπο με τον οποίο τα χειρίζονται. Αφού εντοπίσουν τα προσωπικά τους δεδομένα και πώς ακριβώς τα χρησιμοποιούν, θα πρέπει να τα διασφαλίσουν με τον σωστό τρόπο. Η εξέταση των δεδομένων των ατόμων και πελατών τους από τη σκοπιά της ιδιωτικότητάς τους, από την ανάπτυξη του προϊόντος σε όλη την αλυσίδα του εφοδιασμού έως τον τελικό πελάτη, είναι ακριβώς η ουσία της νέας νομοθεσίας των προσωπικών δεδομένων.

3) Περισσότερα μέσα επιβολής κυρώσεων και προστίμων. Με τον νέο Κανονισμό, η επιβολή του νόμου γίνεται αυστηρότερη. Οι Αρχές Προστασίας Προσωπικών Δεδομένων αποκτούν περισσότερους πόρους και θα ενώσουν τις δυνάμεις τους σε ένα νέο πανευρωπαϊκό σώμα που θα εκδίδει δεσμευτικές γνωμοδοτήσεις. Εκτός αυτού, τα πρόστιμα θα είναι τόσο υψηλά - έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών ενός οργανισμού - που ο νέος Κανονισμός αυτομάτως αφυπνίζει τους οργανισμούς σε όλους τους κλάδους. Ο φόβος της επιβολής προστίμου δεν θα έπρεπε να είναι το βασικό κίνητρο των οργανισμών για

συμμόρφωση, αλλά είναι σίγουρα ένας λόγος για να προσέξουν πολύ περισσότερο, ειδικά στη χώρα μας.

4) Αυξημένη υποχρέωση λογοδοσίας. Ο GDPR καθιστά τους οργανισμούς υπόλογους για την προστασία των προσωπικών δεδομένων. Θα φέρουν το βάρος της απόδειξης όσον αφορά το εάν, το πώς και το πόσο καλά προστάτευσαν τα προσωπικά δεδομένα. Παλαιότερα υπήρχε μια αρκετά τυπική διαδικασία για την απόκτηση άδειας πρόσβασης σε προσωπικά δεδομένα, που βασιζόταν στο είδος των δεδομένων που επεξεργάζονται και στο αν μεταφέρονται σε τρίτους. Σήμερα, αυτό που μετρά περισσότερο θα είναι το πόσο καλά οργανωμένες είναι οι διαδικασίες των επιχειρήσεων, παρά η απόκτηση τυπικής άδειας πρόσβασης. Στο πλαίσιο αυτό, είναι χρήσιμο να υπάρχει κάποιος, είτε εσωτερικά είτε εξωτερικά, που να αντιλαμβάνεται την έννοια του απορρήτου των δεδομένων και να γνωρίζει πώς να επιφέρει αλλαγές και να εφαρμόζει τη νομοθεσία. (Μήτρου , 2017)

Μια άλλη παράμετρος που εισάγει ο νέος Κανονισμός, είναι ότι θεσπίζει ένα νόμο σε ολόκληρη την ήπειρο και ένα ενιαίο σύνολο κανόνων που ισχύουν για τις επιχειρήσεις που αναπτύσσουν επιχειρηματικές δραστηριότητες στην ΕΕ. Αυτό σημαίνει ότι η εμβέλεια της νομοθεσίας εκτείνεται πέρα από τα σύνορα της ίδιας της Ευρώπης, καθώς οι εταιρείες που εδρεύουν εκτός της περιοχής αλλά έχουν δραστηριότητα στο «ευρωπαϊκό έδαφος» θα εξακολουθούν να υπόκεινται σε συμμόρφωση με τον Κανονισμό. Η Ευρωπαϊκή Επιτροπή υποστηρίζει ότι, έχοντας μια ενιαία αρχή εποπτείας για ολόκληρη την ΕΕ, θα καταστεί απλούστερη και φθηνότερη η λειτουργία των επιχειρήσεων στην περιοχή. Αυτό σημαίνει ότι, θα διασφαλιστούν οι εγγυήσεις προστασίας δεδομένων που ενσωματώνονται σε προϊόντα και υπηρεσίες από το αρχικό στάδιο ανάπτυξης, παρέχοντας «προστασία δεδομένων από το σχεδιασμό» σε νέα προϊόντα και τεχνολογίες. Οι οργανισμοί θα ενθαρρυνθούν επίσης να υιοθετήσουν τεχνικές όπως «ψευδωνυμοποίηση» προκειμένου να επωφεληθούν από τη συλλογή και ανάλυση δεδομένων, ενώ ταυτόχρονα προστατεύεται το απόρρητο των πελατών τους.

Επιπρόσθετα, εισάγεται και η υποχρέωση γνωστοποίησης τυχόν παραβιάσεων προσωπικών δεδομένων (data breaches). Όλες οι επιχειρήσεις θα έχουν ως καθήκον να αναφέρουν ορισμένες μορφές παραβιάσεων δεδομένων που συνεπάγονται μη

εξουσιοδοτημένη πρόσβαση ή απώλεια δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή.

Σε ορισμένες περιπτώσεις, οι επιχειρήσεις θα υποχρεούνται να ενημερώνουν τα άτομα που επηρεάζονται από την παραβίαση, ειδικά όταν αυτή ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των ατόμων και να οδηγήσει σε διακρίσεις, οικονομικές απώλειες, απώλεια εμπιστευτικότητας ή οποιοδήποτε άλλο οικονομικό ή κοινωνικό μειονέκτημα. Η γνωστοποίηση απευθύνεται προς την αρμόδια εθνική εποπτική αρχή (άρθρο 33) και σε ορισμένες περιπτώσεις, η παραβίαση πρέπει να ανακοινώνεται και στα άτομα, των οποίων τα προσωπικά δεδομένα έχουν επηρεαστεί από αυτήν (άρθρο 34).

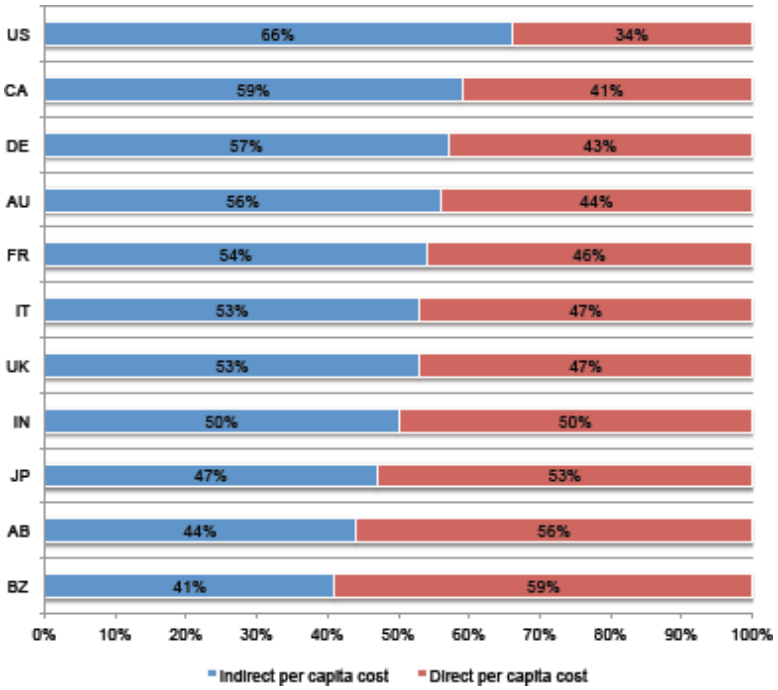
Με άλλα λόγια, σε περίπτωση παραβίασης του ονόματος, της διεύθυνσης, των δεδομένων της γέννησης, των ιατρικών αρχείων, των τραπεζικών στοιχείων ή τυχόν ιδιωτικών δεδομένων σχετικά με τους πελάτες, ο οργανισμός υποχρεούται να ενημερώσει τους ενδιαφερόμενους καθώς και τον αρμόδιο ρυθμιστικό φορέα, για να περιορίσει τη ζημιά

Συνοπτικά, τα άμεσα και έμμεσα κόστη από την εφαρμογή του GDPR, παρουσιάζονται στον ακόλουθο πίνακα:

Τα Άμεσα κόστη περιλαμβάνουν επαγγελματικές αμοιβές εξειδικευμένων συμβούλων διαχείρισης περιστατικών παράβασης συστημάτων, πρόστιμα και έξοδα όπως:	**Τα Έμμεσα κόστη μπορεί να είναι ακόμα πιο σημαντικά για μια επιχείρηση, συμπεριλαμβανομένων:**
✓ αμοιβές εξειδικευμένου δικηγόρου ✓ υπηρεσίες ειδικών ψηφιακής εγκληματολογίας (forensics) ✓ υπηρεσίες δημοσίων σχέσεων και επικοινωνίας ✓ υπηρεσίες τηλεφωνικού κέντρου ✓ υπηρεσίες ελεγκτών ✓ Credit Monitoring – Υπηρεσία Παρακολούθησης χρήσης δεδομένων που έχουν κλαπεί για την πραγματοποίηση παράνομων χρηματοοικονομικών συναλλαγών ✓ έξοδα αντικατάστασης στοιχείων ενεργητικού: α) αντικατάσταση της πιστωτικής κάρτας του πελάτη β) αντικατάσταση υλικού hardware ή software κ.λπ. ✓ έκτακτα έξοδα οπως: α) αναγκαία έξοδα ταξιδιού και διαμονής για ομάδες ειδικών διαχείρισης περιστατικών β) τα έξοδα αποστολής, ενημερωτικών επιστολών σε πελάτες, κ.λ.π., ✓ πρόστιμα για μη τήρηση της νομοθεσίας περί προσωπικών δεδομένων ✓ έξοδα για την επίτευξη επιχειρησιακής συνέχειας ✓ έξοδα εγκατάστασης νέων συστημάτων ασφάλειας	✓ μείωσης της φήμης της εταιρίας ✓ πτώσης των εσόδων ✓ χαμένων επιχειρηματικών ευκαιριών ✓ απώλεια πελατών ✓ απώλεια συνεργατών ✓ καθυστερήσεις έργων και λανσαρίσματος νέων προϊόντων ✓ αύξηση των αμοιβών των υπηρεσιών τρίτων παρόχων ✓ κόστη εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών του ανθρώπινου δυναμικού της εταιρίας ✓ επαναλαμβανόμενα έξοδα για τακτικούς ελέγχους ασφάλειας.

Εικόνα 4: Άμεσα και έμμεσα κόστη από την επιβολή του GDPR στις επιχειρήσεις

Οι επιχειρήσεις, ανησυχούν περισσότερο για τα έμμεσα κόστη και πιο συγκεκριμένα για τη μείωση της φήμης της εταιρείας και την απώλεια των πελατών τους. Εξάλλου όπως περίφημα αναφέρει ο Warren Buffet, χρειάζονται 20 ολόκληρα χρόνια για να χτιστεί η φήμη και πέντε ολόκληρα λεπτά για να καταστραφεί. Στο ακόλουθο σχήμα, παρουσιάζεται το ποσοστιαίο κατά κεφαλήν άμεσο και έμμεσο κόστος της παραβίασης των δεδομένων, όπως παρουσιάστηκαν από το «Ponemon Institute στο Report ”2015 – Cost of Data Breach Study Global Analysis»



Εικόνα 5: Ποσοστιαίο κατά κεφαλήν άμεσο και έμμεσο κόστος της παραβίασης των δεδομένων

3.8 Σύνοψη

Στο παρόν κεφάλαιο, παρουσιάστηκε αναλυτικά ο νέος Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), όπως σχεδιάστηκε και θεσπίστηκε από τα κεντρικά όργανα της Ευρωπαϊκής Ένωσης και τέθηκε σε εφαρμογή στις 25 Μαΐου του 2018 στη χώρα μας. Πραγματοποιήθηκε εκτενής αναφορά, στο περιεχόμενο του νέου αυτού Κανονισμού, καθώς και στις αλλαγές, με την εισαγωγή νέων εννοιών , που επιφέρει σε σχέση με τους προηγούμενους κανονισμούς.

Ακόμη πραγματοποιήθηκε ξεχωριστή αναφορά, στην πολύ σημαντική έννοια της συγκατάθεσης καθώς και στην εισαγωγή ενός νέου όρου και διαδικασίας, της

εκτίμησης αντικτύπου της παραβίασης των προσωπικών δεδομένων, προσαρμοσμένο στην ελληνική πραγματικότητα, με ειδικότερη αναφορά στις ελληνικές επιχειρήσεις, καθώς και στον Δημόσιο τομέα.

Επιπρόσθετα ξεχωριστή αναφορά έγινε στην πολύ αυστηρή επιβολή προστίμων και κυρώσεων, καθώς και σε άλλες επιπτώσεις που προκύπτουν από την εφαρμογή του Κανονισμού, όπως είναι τα άμεσα και έμμεσα κόστη για τις ιδιωτικές επιχειρήσεις. Τέλος ξεχωριστή αναφορά έγινε για το πώς επηρεάζονται τα φυσικά πρόσωπα από τον GDPR, με ειδική αναφορά στην ευαίσθητη ομάδα των παιδιών.

Όλα τα παραπάνω στοιχεία, αποτελούν βασικές και απαραίτητες γνώσεις, για την εξοικείωση με το νέο ρυθμιστικό πλαίσιο που εισάγει ο GDPR, καθώς και για την καλύτερη κατανόηση της μεθοδολογίας και του τρόπου συμμόρφωσης με αυτόν, όπως παρουσιάζονται στο επόμενο κεφάλαιο. Ωστόσο, τον πιο σημαντικό ρόλο της υλοποίησης ου GDPR, έχει ο υπεύθυνος προστασίας δεδομένων, που παρουσιάζεται στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 4 : ΥΠΟΧΡΕΩΤΙΚΟΣ ΟΡΙΣΜΟΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (DPO)

4.1 Εισαγωγή

Η εισαγωγή ενός νέου ανεξάρτητου θεσμού, όπως αυτό του GDPR, ιδίως αν πρόκειται να επιβληθεί υποχρεωτικά όχι μόνο στο Δημόσιο αλλά και στον ιδιωτικό τομέα, κινδυνεύει να μείνει «στα χαρτιά», όπως συμβαίνει με αρκετούς νόμους στη χώρα μας. Η Ευρωπαϊκή Ένωση, θεσπίζοντας το 2016, ύστερα από τετραετείς διαβουλεύσεις, ένα νέο νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων, έχει επενδύσει ιδιαίτερα στην πρακτική εφαρμογή του. Για το λόγο αυτό, έχει επιβάλει τον υποχρεωτικό ορισμό Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO), για μεγάλες κατηγορίες οντοτήτων (υπηρεσιών, επιχειρήσεων και οργανισμών), καθολικά στον δημόσιο τομέα και σημαντικό μέρος του ιδιωτικού τομέα.

Στον παρόν κεφάλαιο, θα γίνει μια εκτενής αναφορά στον υποχρεωτικό διορισμό υπευθύνου προστασίας προσωπικών δεδομένων, στα καθήκοντα με τα οποία θα επιβαρυνθεί και θα πρέπει να φέρεις εις πέρας, καθώς και στα τυπικά προσόντα που απαιτείται να έχει ένα άτομο για να αναλάβει τον πολύ σημαντικό αυτό ρόλο του Υπευθύνου Προστασίας Προσωπικών Δεδομένων σε ένα δημόσιο ή ιδιωτικό οργανισμό.

4.2 Υποχρεωτικός Ορισμός DPO

Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων λειτουργεί εδώ και δεκαετίες σε άλλες χώρες, ως αποκεντρωμένος ανεξάρτητος ελεγκτής για την εφαρμογή των διατάξεων περί προστασίας προσωπικών δεδομένων.

Την υποχρέωση ορισμού Υπευθύνου Προστασία; Προσωπικών Δεδομένων, εφεξής DPO, την έχει ο υπεύθυνος επεξεργασίας (ΥΕ) και ο εκτελών την επεξεργασία (ΕΕ) σε τρεις περιπτώσεις που αναφέρει το άρθρο 37 του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων:

i. Όταν η επεξεργασία πραγματοποιείται από δημόσια αρχή ή οργανισμό,

ii. Όταν οι βασικές δραστηριότητες του ΥΕ ή του ΕΕ συνίστανται σε εργασίες επεξεργασίας, οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των δεδομένων των υποκειμένων σε μεγάλη κλίμακα,

iii. Όταν οι βασικές δραστηριότητες του ΥΕ ή του ΕΕ συνίστανται σε επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων (άρθρο 9) ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα (άρθρο 10).

Η διάταξη του Γενικού Κανονισμού δεν διευκρινίζει ποιες «δημόσιες αρχές ή φορείς» οφείλουν να ορίσουν DPO. Οι δημόσιες αρχές και οι οργανισμοί περιλαμβάνουν εθνικές, περιφερειακές και τοπικές αρχές, αλλά η έννοια, σύμφωνα με την ισχύουσα εθνική νομοθεσία, περιλαμβάνει κατά κανόνα και σειρά άλλων οργανισμών Δημοσίου Δικαίου. Στις περιπτώσεις αυτές, ο καθορισμός ενός DPO είναι υποχρεωτικός.

Ωστόσο, οι «βασικές δραστηριότητες» δεν πρέπει να ερμηνεύονται ως δραστηριότητες στις οποίες η επεξεργασία δεδομένων δεν αποτελεί αναπόσπαστο

μέρος των εργασιών του ΥΕ ή του ΕΕ. Για παράδειγμα, η βασική δραστηριότητα ενός νοσοκομείου είναι η παροχή υγειονομικής περίθαλψης. Ωστόσο, ένα νοσοκομείο δεν θα μπορούσε να παράσχει υγειονομική περίθαλψη με ασφάλεια και αποτελεσματικότητα χωρίς επεξεργασία δεδομένων υγείας, όπως τα αρχεία υγείας των ασθενών. Ως εκ τούτου, η επεξεργασία αυτών των δεδομένων πρέπει να θεωρείται ως μία από τις βασικές δραστηριότητες του νοσοκομείου και επομένως πρέπει να ορισθεί DPO.

Παρόλα αυτά η διάταξη εξαιρεί τα δικαστήρια κατά την ενάσκηση των δικαιοδοτικών τους αρμοδιοτήτων, αφήνοντας έτσι να εννοηθεί όμως ότι για την αρχειακή λειτουργία τους, οι Γραμματείς των Δικαστηρίων οφείλουν να έχουν έναν DPO, διότι η αρχειοθέτηση δεν εντάσσεται στην δικαιοδοτική αρμοδιότητα, αλλά στην διοικητική.

Την υποχρέωση για διορισμό DPO έχουν και ορισμένες κατηγορίες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία στον ιδιωτικό τομέα. Αυτές μπορεί να είναι επιχειρήσεις ή και μη κυβερνητικές οργανώσεις, αστικές εταιρίες μη κερδοσκοπικού χαρακτήρα ή και σωματεία.

Αξίζει να σημειωθεί πως η επέκταση της επιβολής διορισμού στον ιδιωτικό τομέα, αποτελεί μια καινοτομία του Γενικού Κανονισμού.

Η πρώτη λοιπόν κατηγορία υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία στον ιδιωτικό τομέα που οφείλουν να ορίσουν έναν DPO, είναι εκείνες που οι «βασικές δραστηριότητες τους συνιστούν πράξεις επεξεργασίας, οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής ή και των σκοπών τους απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα.[10]. Στο άρθρο 97 του Προοιμίου του Γενικού Κανονισμού, διευκρινίζεται ότι οι «βασικές δραστηριότητες», αφορούν τις «κύριες δραστηριότητες του και όχι την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως παρεπόμενη δραστηριότητα».

Η δεύτερη κατηγορία οντοτήτων του ιδιωτικού τομέα που οφείλουν να ορίσουν έναν DPO είναι εκείνες που η βασική τους δραστηριότητα, είναι η επεξεργασία σε «μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων» και δεδομένων που αφορούν «ποινικές καταδίκες και αδικήματα». Η ορολογία αυτή ουσιαστικά αναφέρεται σε

[10] Άρθρο 37 Παρ.1 του GDPR

αυτά τα δεδομένα, που ο Έλληνας νομοθέτης χαρακτηρίζει ως «ευαίσθητα», όπως είναι η φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα οι θρησκευτικές πεποιθήσεις κ.α.

Ο GDPR δεν καθορίζει τι συνιστά «μεγάλη κλίμακα». Δεν είναι δυνατόν να δοθεί ακριβής αριθμός όσον αφορά το μέγεθος των δεδομένων που υποβλήθηκαν σε επεξεργασία ή τον αριθμό των ενδιαφερομένων. Αυτό δεν αποκλείει, ωστόσο, την πιθανότητα να αναπτυχθεί με την πάροδο του χρόνου μια τυποποιημένη πρακτική για τον ακριβή ποσοτικό προσδιορισμό του τι συνιστά «μεγάλη κλίμακα» όσον αφορά ορισμένες μορφές κοινών δραστηριοτήτων επεξεργασίας.

Η Ομάδα Εργασίας του άρθρου 29, συνιστά να λαμβάνονται ιδιαίτερα υπόψη οι ακόλουθοι παράγοντες για τον καθορισμό του κατά πόσον η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα:

• Ο αριθμός των ενδιαφερόμενων προσώπων στα οποία αναφέρονται τα δεδομένα - είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού.

• Ο όγκος δεδομένων και/ή το φάσμα των διαφορετικών στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία.

• Η διάρκεια ή η μονιμότητα της δραστηριότητας επεξεργασίας δεδομένων.

• Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Παραδείγματα επεξεργασίας μεγάλης κλίμακας περιλαμβάνουν:

• Επεξεργασία δεδομένων ασθενών από νοσοκομείο,

• Επεξεργασία δεδομένων μετακίνησης ατόμων που χρησιμοποιούν το σύστημα δημόσιων συγκοινωνιών της πόλης (π.χ. παρακολούθηση μέσω ηλεκτρονικών καρτών),

• Επεξεργασία δεδομένων γεωγραφικής θέσης σε πραγματικό χρόνο των πελατών μιας διεθνούς αλυσίδας γρήγορου φαγητού για στατιστικούς σκοπούς από εταιρεία ειδικευμένη στην παροχή αυτών των υπηρεσιών,

• Επεξεργασία δεδομένων πελατών από ασφαλιστική εταιρεία ή τράπεζα,

• Επεξεργασία προσωπικών δεδομένων για ανάλυση συμπεριφοράς με σκοπό τη διαφήμιση από μια μηχανή αναζήτησης,

• Επεξεργασία δεδομένων (περιεχόμενο, κίνηση, τοποθεσία) από παρόχους υπηρεσιών Διαδικτύου.

Παραδείγματα που δεν αποτελούν επεξεργασία μεγάλης κλίμακας περιλαμβάνουν:

• Επεξεργασία δεδομένων ασθενών από μεμονωμένο ιατρό,

• Την επεξεργασία προσωπικών δεδομένων σχετικά με ποινικές καταδίκες και αδικήματα από μεμονωμένο δικηγόρο.

Το άρθρο 37 ισχύει τόσο για τους υπευθύνους επεξεργασίας όσο και για τους εκτελούντες την επεξεργασία, όσον αφορά τον ορισμό ενός DPO. Ανάλογα με το ποιος πληροί τα κριτήρια για τον υποχρεωτικό χαρακτηρισμό, τόσο ο υπεύθυνος επεξεργασίας όσο και ο ΕΕ καλούνται να διορίσουν από έναν DPO (οι οποίοι θα πρέπει στη συνέχεια να συνεργάζονται μεταξύ τους). Στην παράγραφο 2 επιτρέπει σε μια ομάδα επιχειρήσεων να ορίσουν έναν ενιαίο DPO υπό τον όρο ότι θα είναι «εύκολα προσβάσιμος από κάθε εγκατάσταση». Η έννοια της προσβασιμότητας αναφέρεται στα καθήκοντα του DPO ως σημείο επαφής σε ότι αφορά τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, την εποπτική αρχή αλλά και εσωτερικά εντός του οργανισμού, θεωρώντας ότι ένα από τα καθήκοντα του DPO είναι «να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας τον ΕΕ και τους υπαλλήλους που πραγματοποιούν την επεξεργασία σύμφωνα με τον παρόντα κανονισμό».

Προκειμένου να διασφαλιστεί η πρόσβαση του DPO, εσωτερικού ή εξωτερικού, είναι σημαντικό να διασφαλιστεί ότι τα στοιχεία επικοινωνίας του είναι διαθέσιμα σύμφωνα με τις απαιτήσεις του GDPR. Ο DPO πρέπει να είναι σε θέση να επικοινωνεί αποτελεσματικά με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις αρμόδιες εποπτικές αρχές. Αυτό σημαίνει επίσης ότι αυτή η επικοινωνία πρέπει να πραγματοποιείται στη γλώσσα ή τις γλώσσες που χρησιμοποιούν οι εποπτικές αρχές και τα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Σύμφωνα με το άρθρο 37 παράγραφος 3, μπορεί να οριστεί ένας DPO για περισσότερες δημόσιες αρχές ή οργανισμούς, λαμβάνοντας υπόψη την οργανωτική δομή και το μέγεθος τους. Ισχύουν τα ίδια σε ότι αφορά τους πόρους και την επικοινωνία.

Η προσωπική διαθεσιμότητα ενός DPO (είτε είναι φυσικά στους ίδιους χώρους όπως οι υπάλληλοι, είτε μέσω ανοικτής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι ουσιαστικής σημασίας για να διασφαλιστεί ότι τα υποκείμενα των δεδομένων θα μπορούν να επικοινωνούν μαζί του. Ο DPO δεσμεύεται από το απόρρητο ή την εμπιστευτικότητα όσον αφορά την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους[11]. Η υποχρέωση τήρησης απορρήτου ή εμπιστευτικότητας δεν εμποδίζει τον DPO να επικοινωνεί και να ζητεί συμβουλές από την εποπτική αρχή. (Σωτηρόπουλος Β. , 2017)

4.3 Προσόντα διορισμού ενός DPO

Ένας DPO διορίζεται «βάσει επαγγελματικών προσόντων και, ειδικότερα, των γνώσεων του σχετικά με τη νομοθεσία και τις πρακτικές προστασίας δεδομένων και την ικανότητα εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39». Το απαιτούμενο επίπεδο ειδικών γνώσεων πρέπει να καθορίζεται ανάλογα με τις διεργασίες επεξεργασίας δεδομένων που πραγματοποιούνται και την προστασία που απαιτείται για την επεξεργασία των προσωπικών δεδομένων.

Παρόλο που το άρθρο 37 παράγραφος 5 δεν διευκρινίζει τις επαγγελματικές ιδιότητες-τυπικά προσόντα που πρέπει να λαμβάνονται υπόψη κατά τον ορισμό του DPO, είναι σημαντικό το γεγονός ότι οι DPO πρέπει να έχουν πείρα σε εθνικές και ευρωπαϊκές νομοθεσίες και πρακτικές για την προστασία των δεδομένων, καθώς και να έχουν κατανοήσει σε βάθος τον GDPR. Η «εμπειρογνωσία» στο δίκαιο και τις πρακτικές της προστασίας των προσωπικών δεδομένων δεν μπορεί να πιστοποιείται με βεβαιότητα σε άτομα με άλλο μορφωτικό υπόβαθρο, στο οποίο δεν αποκλείεται μεν να έχει αποκτηθεί εξοικείωση με την προστασία των προσωπικών δεδομένων, σίγουρα όμως όχι ως προς την νομική της διάσταση. Σημειωτέων πάντως ότι ο GDPR δεν επιβάλλει κάποιου είδους «πιστοποίηση» για να γίνει κάποιος DPO. Ωστόσο είναι επίσης χρήσιμο οι εποπτικές αρχές να βοηθήσουν στην επαρκή και τακτική κατάρτιση για τους Υπευθύνους Προσωπικών Δεδομένων.

Η γνώση του επιχειρηματικού τομέα και της οργάνωσης του υπεύθυνου επεξεργασίας είναι χρήσιμη. Ο DPO πρέπει επίσης να έχει επαρκή κατανόηση των

[11] Άρθρο 38Παρ. 5

διεξαγόμενων εργασιών επεξεργασίας, καθώς και των συστημάτων πληροφοριών και των απαιτήσεων ασφάλειας και προστασίας των δεδομένων του υπεύθυνου επεξεργασίας.

Στην περίπτωση δημόσιας αρχής ή φορέα, ο DPO πρέπει επίσης να έχει καλή γνώση των διοικητικών κανόνων και διαδικασιών του οργανισμού.

Ο πρωταρχικός στόχος του DPO πρέπει να είναι η συμμόρφωση με το GDPR. Ο DPO διαδραματίζει βασικό ρόλο στην καλλιέργεια μιας κουλτούρας ασφάλειας και προστασίας των δεδομένων εντός του οργανισμού και συμβάλλει στην υλοποίηση των βασικών αρχών του GDPR, όπως οι αρχές επεξεργασίας δεδομένων, τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα, η προστασία δεδομένων από το σχεδιασμό και εξ ορισμού, τα αρχεία των δραστηριοτήτων επεξεργασίας, την ασφάλεια της επεξεργασίας και την αναγγελία των παραβιάσεων των δεδομένων.

Ο ρόλος του DPO μπορεί επίσης να ασκείται βάσει σύμβασης παροχής υπηρεσιών που συνάπτεται με ιδιώτη ή οργανισμό εκτός του οργανισμού του υπεύθυνου επεξεργασίας.

Το άρθρο 37 παράγραφος 7 του GDPR απαιτεί από τον υπεύθυνο επεξεργασίας ή τον εκτελών την επεξεργασία:

- Να δημοσιεύσει τα στοιχεία επικοινωνίας του DPO,
- Να κοινοποιήσει τα στοιχεία επικοινωνίας στις αρμόδιες εποπτικές αρχές.

Στόχος αυτών των απαιτήσεων είναι να διασφαλιστεί ότι τα υποκείμενα των δεδομένων (εντός και εκτός του οργανισμού) και οι εποπτικές αρχές μπορούν να επικοινωνούν εύκολα, άμεσα και εμπιστευτικά με τον DPO χωρίς να χρειάζεται να έρθουν σε επαφή με άλλο τμήμα του οργανισμού.

Τα στοιχεία επικοινωνίας του DPO πρέπει να περιλαμβάνουν πληροφορίες που επιτρέπουν στα υποκείμενα των δεδομένων και στις εποπτικές αρχές να φτάσουν στον DPO με εύκολο τρόπο (ταχυδρομική διεύθυνση, αποκλειστικός τηλεφωνικός αριθμός και ειδική διεύθυνση ηλεκτρονικού ταχυδρομείου). Όπου ενδείκνυται, για σκοπούς επικοινωνίας με το κοινό, θα μπορούσαν επίσης να παρασχεθούν και άλλα

μέσα επικοινωνίας, για παράδειγμα, ειδική τηλεφωνική γραμμή ή ειδική φόρμα επικοινωνίας στον ιστότοπο του οργανισμού για τον DPO.

Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να συμμετέχει από το αρχικό στάδιο σε όλα τα ζητήματα που αφορούν την προστασία των δεδομένων. Επιπλέον, είναι σημαντικό ο DPO να θεωρείται εταίρος συζήτησης στο πλαίσιο του οργανισμού και ότι αυτός ή αυτή αποτελεί μέρος των σχετικών ομάδων εργασίας που ασχολούνται με δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού.

Κατά συνέπεια, ο οργανισμός πρέπει να διασφαλίσει, ότι:

- Ο DPO καλείται να συμμετέχει τακτικά σε συνεδριάσεις ανώτερων και μεσαίων στελεχών.

- Συνιστάται η παρουσία του/της DPO όταν λαμβάνονται αποφάσεις με συνέπειες στην προστασία δεδομένων. Όλες οι σχετικές πληροφορίες πρέπει να διαβιβάζονται έγκαιρα προκειμένου να του επιτρέψουν να παρέχει επαρκείς συμβουλές.

- Πρέπει πάντοτε να λαμβάνεται υπόψη η γνώμη του DPO. Σε περίπτωση διαφωνίας, η ομάδα εργασίας του άρθρου 29 συνιστά, ως ορθή πρακτική, να τεκμηριωθούν οι λόγοι για τους οποίους δεν ακολουθήθηκε η συμβουλή του DPO.

- Ο υπεύθυνος προστασίας δεδομένων πρέπει να ενημερώνεται αμέσως μόλις έχει σημειωθεί παραβίαση δεδομένων ή άλλο περιστατικό.

Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα μπορούσε να αναπτύξει κατευθυντήριες γραμμές ή προγράμματα σχετικά με την προστασία δεδομένων, τα οποία καθορίζονται όταν πρέπει να συμβουλευτεί ο DPO.

Το άρθρο 38 παράγραφος 2 του GDPR απαιτεί από τον οργανισμό να υποστηρίζει τον DPO του με «την παροχή των αναγκαίων πόρων για την εκτέλεση των καθηκόντων του και την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και τις εργασίες επεξεργασίας και για τη διατήρηση των ειδικών γνώσεων του». Ειδικότερα, πρέπει να λαμβάνονται υπόψη τα εξής:

- Ενεργός υποστήριξη της λειτουργίας του DPO από ανώτατα στελέχη (όπως σε επίπεδο διοικητικών συμβουλίων).

• Ένας επαρκής χρόνος για να εκπληρώσουν τα καθήκοντά τους οι DPO. Αυτό είναι ιδιαίτερα σημαντικό όταν ο DPO διορίζεται με μερική απασχόληση ή ασκεί και άλλα καθήκοντα. Διαφορετικά, οι αντικρουόμενες προτεραιότητες θα μπορούσαν να οδηγήσουν στην παραμέληση των καθηκόντων του DPO.

• Επαρκής στήριξη όσον αφορά τους οικονομικούς πόρους, την υποδομή (χώρους, εγκαταστάσεις, εξοπλισμό) και το προσωπικό, όπου ενδείκνυται.

• Επίσημη ανακοίνωση του ορισμού του DPO σε όλο το προσωπικό, ώστε να διασφαλιστεί ότι η ύπαρξή του και η λειτουργία του είναι γνωστά στον οργανισμό.

• Απαραίτητη πρόσβαση σε άλλες υπηρεσίες, όπως το Ανθρώπινο Δυναμικό, τη Νομική Υπηρεσία, την Πληροφορική, την Ασφάλεια κ.λπ., ώστε οι DPO να μπορούν να λαμβάνουν ουσιαστική υποστήριξη και πληροφορίες από αυτές τις υπηρεσίες.

• Συνεχής εκπαίδευση. Οι DPO πρέπει να έχουν τη δυνατότητα να ενημερώνονται σχετικά με τις εξελίξεις στον τομέα της προστασίας δεδομένων. Θα πρέπει να ενθαρρυνθούν να συμμετάσχουν σε μαθήματα κατάρτισης σχετικά με την προστασία των δεδομένων και άλλες μορφές επαγγελματικής ανάπτυξης, όπως η συμμετοχή σε φόρουμ για την προστασία της ιδιωτικής ζωής, σε εργαστήρια κ.λπ.

• Δεδομένου του μεγέθους και της διάρθρωσης της οργάνωσης, μπορεί να χρειαστεί να δημιουργηθεί μια Ομάδα Προστασίας Προσωπικών Δεδομένων (ο DPO και το αντίστοιχο προσωπικό). Σε τέτοιες περιπτώσεις, η εσωτερική δομή της ομάδας και τα καθήκοντα και οι αρμοδιότητες κάθε μέλους της πρέπει να καταρτίζονται σαφώς. Ομοίως και όταν η λειτουργία του DPO ασκείται από εξωτερικό πάροχο υπηρεσιών.

• Το άρθρο 38 παράγραφος 3 θεσπίζει ορισμένες βασικές εγγυήσεις για να διασφαλίσει ότι οι DPO είναι σε θέση να εκτελούν τα καθήκοντά τους αυτόνομα εντός του οργανισμού. Ειδικότερα, οι υπεύθυνοι επεξεργασίας ή ο εκτελών την επεξεργασία καλούνται να διασφαλίσουν ότι ο DPO «δεν λαμβάνει οδηγίες σχετικά με την άσκηση των καθηκόντων του». Αυτό σημαίνει ότι, κατά την εκπλήρωση των καθηκόντων τους βάσει του άρθρου 39, οι DPO δεν πρέπει να «κατευθύνονται» για το πώς να χειριστούν ένα θέμα, για παράδειγμα ποιο αποτέλεσμα πρέπει να επιτευχθεί, πώς να διερευνήσει μια καταγγελία ή αν πρέπει να συμβουλευθεί την

εποπτική αρχή. Επιπλέον, δεν πρέπει να τους δοθεί η εντολή να λάβουν ορισμένη άποψη/απόφαση σχετικά με ένα ζήτημα που σχετίζεται με το δίκαιο προστασίας των δεδομένων, για παράδειγμα, μια συγκεκριμένη ερμηνεία του νόμου.

Το άρθρο 38, παράγραφος 3, επιβάλλει επίσης ότι οι DPO «δεν πρέπει να απορρίπτονται ή να τιμωρούνται από τον υπεύθυνο επεξεργασίας ή τον εκτελών την επεξεργασία για την εκτέλεση των καθηκόντων του». Η απαίτηση αυτή ενισχύει επίσης την αυτονομία των DPO και διασφαλίζει ότι ενεργούν ανεξάρτητα και απολαμβάνουν επαρκούς προστασίας κατά την εκτέλεση των καθηκόντων τους για την προστασία των δεδομένων.

Η έλλειψη σύγκρουσης συμφερόντων συνδέεται στενά με την απαίτηση ο DPO να ενεργεί με ανεξάρτητο τρόπο. Οι DPO επιτρέπεται να ασκούν και άλλες λειτουργίες, μόνον εφόσον δεν δημιουργούνται συγκρούσεις συμφερόντων. Αυτό συνεπάγεται ειδικότερα ότι ο DPO δεν μπορεί να κατέχει θέση εντός του οργανισμού που τον οδηγεί να προσδιορίσει τους σκοπούς και τα μέσα επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Λόγω της συγκεκριμένης οργανωτικής δομής σε κάθε οργανισμό, αυτό πρέπει να λαμβάνεται υπόψη κατά περίπτωση.

Τέλος για τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία προτείνεται:

- Να προσδιορίσουν τις θέσεις που θα ήταν ασυμβίβαστες με τη λειτουργία του DPO,
- Να εκπονήσουν εσωτερικούς κανόνες για το σκοπό αυτό, προκειμένου να αποφευχθούν συγκρούσεις συμφερόντων,
- Να συμπεριλάβουν διασφαλίσεις στους εσωτερικούς κανόνες του οργανισμού και να διασφαλίσουν ότι η προκήρυξη κενής θέσης για τη θέση του DPO είναι επαρκώς ακριβής και λεπτομερής προκειμένου να αποφευχθεί η σύγκρουση συμφερόντων. Στο πλαίσιο αυτό, πρέπει επίσης να ληφθεί υπόψη ότι οι συγκρούσεις συμφερόντων μπορούν να λάβουν διάφορες μορφές ανάλογα με το εάν ο DPO προσλαμβάνεται εσωτερικά ή εξωτερικά. (Σωτηρόπουλος Β. , 2017) (Carey , 2018)

4.4 Καθήκοντα ενός DPO

Τα καθήκοντα του DPO μνημονεύονται σε πέντε υποπαραγράφους στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων. Ένας κανόνας που αφορά γενικά την εκτέλεση των καθηκόντων του DPO περιλαμβάνεται στην παράγραφο 2 του άρθρου 39 του GDPR. Σύμφωνα με τη διάταξη αυτή κατά την εκτέλεση των καθηκόντων του ο DPO, «λαμβάνει δεόντως υπόψιν του τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας». Ουσιαστικά επιβάλει στους DPO να θελήσουν προτεραιότητες στις δραστηριότητές τους και να εστιάσουν τις προσπάθειές τους σε θέματα τα οποία παρουσιάζουν αυξημένους κινδύνους για την προστασία των προσωπικών δεδομένων. Αυτό δεν σημαίνει ότι πρέπει να αμελούν την παρακολούθηση συμμόρφωσης για τις επεξεργασίες δεδομένων που έχουν λιγότερα επίπεδα κινδύνου, αλλά υποδεικνύει ότι πρέπει να εστιάσουν αρχικά στις περιοχές με τον μεγαλύτερο κίνδυνο. (Σωτηρόπουλος Β. , 2017)

Αυτή η επιλεκτική και πραγματική προσέγγιση θα μπορούσε να συντρέξει τους DPO να συμβουλεύσουν τους υπεύθυνους επεξεργασίας ως προς την μεθοδολογία που πρέπει να χρησιμοποιήσουν κατά την διενέργεια της εκτίμησης αντικτύπου, ποιες περιοχές πρέπει να υποβάλλονται σε εξωτερικό ή εσωτερικό έλεγχο προστασίας δεδομένων, ποιες εσωτερικές εκπαιδευτικές δράσεις χρειάζονται για το προσωπικό και τα στελέχη που είναι υπεύθυνα για τις επεξεργασίες δεδομένων και σε ποιες επεξεργασίες δεδομένων πρέπει να αφιερωθεί περισσότερος χρόνος και πόροι. Ακόμη ο κανόνας αυτός μπορεί να βοηθήσει τους DPO κατά την κατάρτιση ετήσιου προγράμματος εργασιών, η σύνταξη του οποίου αποτελεί μια από τις βέλτιστες πρακτικές σύμφωνα με τα «Επαγγελματικά πρότυπα των DPO που υπηρετούν στα κοινοτικά όργανα».

Επιγραμματικά τα καθήκοντα ενός DPO είναι:

- ✓ Να παρέχει ενημέρωση και συμβουλές, τόσο στον υπεύθυνο επεξεργασίας, όσο και στον εκτελούντα την επεξεργασία σχετικά με νέες ή υφιστάμενες αρχές που απορρέουν τόσο από τον GDPR, όσο και από νέους νόμους και εξελίξεις στον τομέα των προσωπικών δεδομένων. Επίσης να ενημερώνει σχετικά με τις διατάξεις που

ρυθμίζουν την έκταση και τις προϋποθέσεις της ευθύνης του υπεύθυνου επεξεργασίας.

- ✓ Να προβαίνει σε εκτίμηση αντικτύπου, δηλαδή να παρέχει συμβουλές όταν του ζητείται όσον αφορά την εκτίμηση του αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων και να παρακολουθεί την υλοποίησή της, καθώς και να ενημερώνει τον οργανισμό για τις περιοριστικά απαριθμούμενες περιστάσεις υπό τις οποίες επιτρέπεται η επεξεργασία των δεδομένων.[12]
- ✓ Να ενημερώνει τον οργανισμό για τους κανόνες που διέπουν τις αρχές της συλλογής και επεξεργασίας, και συγκεκριμένα την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας των δεδομένων, την αρχή του περιορισμού της περιόδου αποθήκευσης των δεδομένων, την αρχή της ακεραιότητας και εμπιστευτικότητας και την αρχή της λογοδοσίας, καθώς και την ευθύνη του υπευθύνου επεξεργασίας να αποδείξει την συμμόρφωση του με τις ανωτέρων αρχές.
- ✓ Να ενημερώνει για τις ειδικές ρυθμίσεις που προβλέπονται στα άρθρα 7 και 8 του GDPR για την νόμιμη συγκατάθεση του υποκειμένου των δεδομένων
- ✓ Να ενημερώνει τους ιθύνοντες για τις απαγορεύσεις επεξεργασίας ευαίσθητων προσωπικών δεδομένων και για τις περιπτώσεις που επιτρέπεαι η επεξεργασία τους
- ✓ Να συνεργάζεται και να διαβουλεύεται με την εποπτική Αρχή, δηλαδή να ενεργεί ως σημείο επικοινωνίας με την Αρχή για ζητήματα που σχετίζονται με την επεξεργασία προσωπικών δεδομένων. Ο DPO οφείλει στα πλαίσια των καθηκόντων του να ζητήσει την γνώμη της Αρχής πριν από την επεξεργασία, όταν η εκτίμηση του αντικτύπου σχετικά με την προστασία των δεδομένων θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.
- ✓ Να καταγράφει τις γνωμοδοτήσεις και τα κείμενα που δημοσιεύει η Ομάδα εργασίας τους άρθρου 29, που μετεξελίσσεται σε Ευρωπαϊκό Συμβούλιο Προστασίας Προσωπικών Δεομένων, ώστε να ενημερώνεται για την ενιαία ερμηνεία των όρων και των κανόνων που περιλαμβάνονται στον GDPR
- ✓ Να παρακολουθεί ημερίδες, συνέδρια που διοργανώνονται σχετικά με την προστασία προσωπικών δεδομένων, κάτι που προβλέπεται από το θεσμικό πλαίσιο

Ωστόσο το βασικότερο καθήκον ενός DPO είναι η παρακολούθησης της συμμόρφωσης με τον GDPR.

[12] (Άρθρο παρ. του GDPR και άρθρο 34 στοιχείο γ της Οδηγίας (ΕΕ) 2016/680

Κατά την Ομάδα Εργασίας του άρθρου 29, η παρακολούθηση της συμμόρφωσης δεν σημαίνει ότι ο DPO είναι προσωπικά υπεύθυνος όταν υπάρχει ένα περιστατικό μη συμμόρφωσης. Ο GDPR καθιστά σαφές ότι απαιτείται από τον υπεύθυνο επεξεργασίας και όχι από τον DPO, να «εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει και να αποδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον παρόντα κανονισμό». Η συμμόρφωση με την προστασία δεδομένων αποτελεί εταιρική ευθύνη του υπεύθυνου επεξεργασίας των δεδομένων και όχι του DPO. Ωστόσο ο DPO οφείλει να παρακολουθεί την συμμόρφωση με τον GDPR και να μην αποστασιοποιείται από αυτήν. Περαιτέρω του βασικού καθήκοντος του DPO ως προς την παρακολούθηση της συμμόρφωσης πρέπει να έχει τουλάχιστον τα ακόλουθα:

- Την συλλογή πληροφοριών για να καθοριστούν οι επεξεργασίες δεδομένων.
- Την ανάλυση και τον έλεγχο της συμμόρφωσης ως προς τις επεξεργασίες δεδομένων
- Την πληροφόρηση, παροχή συμβουλών και έκδοση συστάσεων προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.
- Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. (Κοτσαλής & Μενουδάκος , 2018) (Voigt & Bussche , 2017)

4.5 Σύνοψη

Στο παρόν κεφάλαιο, αναπτύχθηκε διεξοδικά μια νέα έννοια που εισήχθη με την εφαρμογή του GDPR, αυτή του υπευθύνου προστασίας προσωπικών δεδομένων (DPO). Αναλύθηκαν εκτενώς, ποιοι είναι και για ποιους λόγους υπόχρεοι στο ορισμό DPO στις οικονομικές τους οντότητες ανεξαρτήτως νομικού τύπου, δημόσιες ή ιδιωτικές. Ακόμη αναλύθηκαν όλα τα ελάχιστα τυπικά προσόντα που πρέπει να κατέχει ένα άτομο για να οριστεί ως DPO, καθώς και τα πολύ σημαντικά καθήκοντα που πρέπει να επωμιστεί και να φέρει εις πέρας, όχι μόνο ως προς την συμμόρφωση

και τήρηση των κανόνων του νέου Κανονισμού, αλλά και ως προς την δια βίου ενασχόλησή του με το αντικείμενο της προστασίας των προσωπικών δεδομένων, και των νέων διατάξεων που θα βγουν στο μέλλον.

Ουσιαστικά ο υπεύθυνος προστασίας προσωπικών δεδομένων (DPO), πρόκειται για μια νέα επαγγελματική κατηγορία, ένα νέο που εισήχθη με τον GDPR, όπου όμως απαιτεί πολλά τυπικά προσόντα, καθώς και μεγάλη προσοχή και εχεμύθεια. Το να αποφασίσει κάποιος να ακολουθήσει αυτό το νέο επάγγελμα θα πρέπει να είναι μια συνειδητή απόφαση, που θα απαιτεί συνεχής ενημέρωση και εξοικείωση στο θέμα της προστασίας των προστασίας των προσωπικών δεδομένων, καθώς και μεγάλη προσοχή και τήρηση των κανόνων του GDPR, για την αποφυγή επιβολής υψηλών προστίμων στον οργανισμό που είναι υπεύθυνος. Ο DPO θα πρέπει να έχει τις βασικές και απαραίτητες γνώσεις ώστε να εξοικειωθεί με το νέο ρυθμιστικό πλαίσιο που εισάγει ο GDPR, ώστε να βοηθήσει τους ιθύνοντες του οργανισμού για την καλύτερη κατανόηση της μεθοδολογίας και του τρόπου συμμόρφωσης με αυτόν, όπως παρουσιάζονται στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 5 : ΜΕΘΟΔΟΛΟΓΙΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

5.1 Εισαγωγή

Όπως έχει ειπωθεί και πιο πάνω, ο Γενικός Κανονισμός Προσωπικών Δεδομένων (GDPR), έχει τεθεί σε υποχρεωτική εφαρμογή στη χώρα μας στις 25 Μαΐου του 2018. Τα πρόστιμα είναι αρκετά υψηλά για κάποια οντότητα ιδιωτική ή δημόσια που δεν θα συμμορφωθεί, όμως δεν υπάρχει κανένας λόγος για πανικό. Όπως και η ίδια η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει, και ορθώς, επισημάνει ότι η 25 Μαΐου 2018 δεν αποτελεί το τέλος αλλά την αρχή μιας διαδικασίας προσαρμογής. Επομένως, τα αρκετά υψηλά πρόστιμα που προβλέπει ο Κανονισμός μπορούν να περιμένουν, προς ώρας τουλάχιστον. Εντούτοις, οι οικονομικές οντότητες δεν θα πρέπει να εφησυχάζουν.

Κάθε οντότητα, θα πρέπει να επενδύσει σε πόρους υλικούς και ανθρώπινους. Να λάβει δηλαδή κάποια μέτρα, ή αλλιώς να κάνει μια προεργασία που θα την οδηγήσει στην επιτυχή συμμόρφωση με τον Κανονισμό, και στην αποφυγή της επιβολής προστίμων. Αυτά τα μέτρα-κανόνες που θα πρέπει να ακολουθήσει κάθε οντότητα ανεξαρτήτου μορφής δημόσιας ή ιδιωτικής, είναι μοναδικά και δεν μπορούν να αντιγραφούν από άλλους οργανισμούς. Κάθε επιχείρηση θα πρέπει πρώτα να εξετάσει τι ακριβώς απαιτείται για να επιτευχθεί η συμμόρφωση με τον νέο αυτό Κανονισμό, λαμβάνοντας υπόψιν της το μέγεθος της αλλά και τα προσωπικά στοιχεία που είναι συγκεντρωμένα στην επιχείρηση καθώς και να ορίσει ποιος θα είναι ο Υπεύθυνος Προσωπικών της Δεδομένων (DPO), ο οποίος θα πρέπει να συνεργαστεί με τον υπεύθυνο επεξεργασίας, ο οποίος θα επιβαρυνθεί με την ευθύνη της συμμόρφωσης με τον Κανονισμό.

Οι κανόνες αυτοί, πρέπει πρώτα απ' όλα να ελαχιστοποιήσουν τον κίνδυνο παραβίασης και να προασπίσουν την προστασία των προσωπικών δεδομένων. Στην έννοια των νέων αυτών μέτρων, όπως γίνεται αντιληπτό εμπεριέχονται περισσότερες πολιτικές και διαδικασίες για τους οργανισμούς, που ισοδυναμεί από τη μια με περισσότερο φόρτο εργασίας για τους υπαλλήλους, είτε για έναν υπάλληλο σε μια μικρή επιχείρηση, είτε ενός ολόκληρου τμήματος σε έναν όμιλο και από την άλλη περισσότερες δαπάνες και επιβάρυνση του προϋπολογισμού με την υιοθέτηση εφαρμογών διακυβέρνησης για την διοίκηση της εκάστοτε οντότητας.

Όπως ορίζεται και στις διατάξεις του GDPR, οι επιχειρήσεις πρέπει να εφαρμόσουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων, όπως κατάρτιση και εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων των δραστηριοτήτων επεξεργασίας και ανασκόπηση των πολιτικών ανθρώπινου δυναμικού, καθώς και τήρηση τεκμηρίωσης σχετικά με τις δραστηριότητες επεξεργασίας. Ακόμη οι οργανισμοί μπορούν να συμπεριλάβουν την ψευδωνυμοποίηση και την ελαχιστοποίηση των δεδομένων, καθώς και την παροχή ειδικής άδειας σε καταρτισμένα άτομα να παρακολουθούν την διαδικασία.

Στο παρόν κεφάλαιο θα γίνει μια προσπάθεια προσέγγισης του χρονοδιαγράμματος και των διαδικασιών συμμόρφωσης των επιχειρήσεων με τον GDPR καθώς και των πρακτικών που μπορούν να ακολουθήσουν για να προετοιμαστούν κατάλληλα για την νέα εποχή όσον αφορά τα προσωπικά δεδομένα.

5.2 Βήματα συμμόρφωσης με τον GDPR

Βασική απαίτηση του νέου περιβάλλοντος που καλούνται να δραστηριοποιηθούν οι επιχειρήσεις αλλά και οι δημόσιοι οργανισμοί είναι η κατάλληλη προετοιμασία και συμμόρφωσή τους με το νέο Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR). Οι οντότητες που είναι υπόχρεοι προς την συμμόρφωσή τους με τον νέο Κανονισμό, οφείλουν να επιλέγουν προϊόντα και υπηρεσίες προστασίας για τις πληροφορίες που διαχειρίζονται, τα οποία θα τις βοηθήσουν να αντιμετωπίσουν αποτελεσματικότερα τυχόν μελλοντικά περιστατικά, δημιουργώντας έτσι τις κατάλληλες συνθήκες που θα εξασφαλίσουν την ασφάλεια των εταιριών και την ανάπτυξη στην αγορά της «κυβερνοασφάλειας».

Οι οργανισμοί, θα πρέπει να λάβουν υπόψιν τους, τα δικαιώματα των υποκειμένων των δεδομένων για την προστασία των προσωπικών τους στοιχείων και οφείλουν να μεριμνήσουν για την αποτελεσματικότερη ανταπόκρισή τους σε αυτά. Πιο συγκεκριμένα, κάθε επιχείρηση και οργανισμός, θα πρέπει να γνωρίζει :

- ✓ Το δικαίωμα στη **«λήθη»** και τις ενέργειες που πρέπει να ακολουθήσει όταν ένα άτομο ζητά τη διαγραφή των δεδομένων του από το αρχείο της
- ✓ Το δικαίωμα **περιορισμού της επεξεργασίας** και τις περιπτώσεις στις οποίες οφείλει να αναπροσαρμόζει την επεξεργασία των προσωπικών δεδομένων των υποκειμένων.
- ✓ Το δικαίωμα στη **φορητότητα των δεδομένων** και τη μορφή στην οποία θα πρέπει να δίνει αντίγραφα όταν το υποκείμενο ζητά πρόσβαση στα δεδομένα του.
- ✓ Τους **περιορισμούς** στην κατάρτιση προφίλ και τις καταστάσεις στις οποίες θα επιτρέπεται η δημιουργία «προφίλ» για το υποκείμενο των δεδομένων.
- ✓ Τις **περιστάσεις** στις οποίες η επιχείρηση οφείλει να ενημερώνει το υποκείμενο των δεδομένων ότι πραγματοποιήθηκε παραβίαση των δεδομένων του.

Για να μπορέσουν συνεπώς οι οικονομικές οντότητες να ανταπεξέλθουν στα νέα αυτά δεδομένα που εισάγει ο νέος Κανονισμός, θα πρέπει αρχικά να ακολουθήσουν κάποια βήματα προετοιμασίας, ή όπως ορίζει ο νόμος, κάποια βήματα συμμόρφωσης όπως:

1) **Διαμόρφωση συνείδησης προστασίας προσωπικών δεδομένων στην επιχείρηση**(awareness). Αυτό προϋποθέτει ενημέρωση όχι μόνο της διοίκησης αλλά και όλου του προσωπικού για το ότι ο Κανονισμός επιφέρει αλλαγές στην προστασία των δεδομένων και κατ' επέκταση, ενδεχομένως, και στη λειτουργία της επιχείρησης. Συνεπώς, όλοι οι εργαζόμενοι επιβάλλεται να γνωρίζουν, στο βαθμό που είναι αναγκαίο για την ορθή άσκηση των καθηκόντων τους, τί επιτρέπεται και τί απαγορεύεται, τί είναι υποχρεωτικό και τί προαιρετικό, με βάση τον Κανονισμό. Ακόμη και αν όλα τα τεχνικά μέτρα προστασίας που η επιχείρηση εφαρμόζει είναι άψογα, εφόσον δεν υπάρξει ευαισθητοποίηση και κινητοποίηση του ανθρώπινου δυναμικού της, θα ανακύπτουν συνεχώς προβλήματα συμμόρφωσης.

2) **Χαρτογράφηση των προσωπικών δεδομένων** τα οποία η επιχείρηση επεξεργάζεται, τις πηγές από τις οποίες τα αντλεί και τους αποδέκτες τους. Ανάλογα με την περίπτωση, είναι πιθανό να απαιτείται ένας ενδελεχής πληροφορικός έλεγχος (information audit). Θα πρέπει να γίνει καταγραφή των δραστηριοτήτων του οργανισμού που εμπίπτουν στον Κανονισμό, ούτως ώστε να διευκολύνεται τόσο η εσωτερική λειτουργία του οργανισμού όσο και η εφαρμογή των αρχών της Δ\διαφάνειας και της λογοδοσίας. Οι υπεύθυνοι επεξεργασίας επωμίζονται με την υποχρέωση της συμμόρφωσης με τον Κανονισμό αλλά και την υποχρέωση να επιδεικνύουν τη συμμόρφωσή τους αυτή.

3) **Αναθεώρηση της πολιτικής απορρήτου** (γνωστή και ως πολιτική προστασίας δεδομένων, privacy notice) ώστε να είναι συμβατή με τις διατάξεις του Κανονισμού. Προκειμένου η πολιτική απορρήτου να καταστεί όσο γίνεται περισσότερο προσπελάσιμη και ευρύτερα γνωστή, συνιστάται η ανάρτησή της στην αρχική ιστοσελίδα της επιχείρησης. Οι υπεύθυνοι επεξεργασίας, εκτός της ταυτότητάς τους και του τρόπου με τον οποίο σκοπεύουν να χρησιμοποιήσουν τα προσωπικά δεδομένα που συλλέγουν, υποχρεώνονται πλέον από τον Κανονισμό να γνωστοποιούν στο υποκείμενο των δεδομένων τη νόμιμη βάση επεξεργασίας των δεδομένων του, το χρόνο τήρησής τους και το δικαίωμά του για υποβολή καταγγελίας στην αρμόδια εποπτική αρχή. Η πληροφόρηση πρέπει πάντα να γίνεται σε ύφος "λακωνικό" (όχι υπερπληροφόρηση) και σε γλώσσα σαφή και εύκολα κατανοητή στο μέσο πολίτη

4) **Έλεγχος των υφιστάμενων διαδικασιών της επιχείρησης** ώστε να εξακριβωθεί αν και κατά πόσο τα νέα δικαιώματα επηρεάζουν τις δραστηριότητες του οργανισμού και να συζητήσουν με το προσωπικό τους, τους τρόπους με τους οποίους

οι πολίτες θα μπορούν να ασκούν τα δικαιώματά τους. Με τον όρο νέα δικαιώματα που δημιουργεί ο GDPR αναφερόμαστε στα:

- Δικαιώματα ενημέρωσης
- Δικαιώματα πρόσβασης
- Δικαιώματα διόρθωσης
- Δικαιώματα διαγραφής (το λεγόμενο «δικαίωμα στη λήθη»)
- Δικαιώματα στον περιορισμό της επεξεργασίας
- Δικαιώματα στη φορητότητα των δεδομένων
- Δικαιώματα εναντίωσης
- Δικαιώματα στην ανθρώπινη παρέμβαση

Για παράδειγμα:

Σε περίπτωση που ένα υποκείμενο δεδομένων ζητά από μια επιχείρηση να διαγράψει τα προσωπικά του δεδομένα από τα αρχεία της, προκύπτουν οι εξής ερωτήσεις:

- Έχει λάβει η επιχείρηση τα κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να είναι σε θέση κατ' αρχάς να εντοπίσει και στη συνέχεια να διαγράψει τα δεδομένα του συγκεκριμένου υποκειμένου;
- Έχει ορίσει το άτομο ή την ομάδα που θα έχει την αποφασιστική αρμοδιότητα περί διαγραφής ή μη;

Ακόμη όσον αφορά την φορητότητα, αν η επιχείρηση προβαίνει σε αυτοματοποιημένη επεξεργασία δεδομένων με βάση σύμβαση ή τη συγκατάθεση του υποκειμένου, οφείλει να ελέγξει και αναλόγως να αναθεωρήσει τις διαδικασίες της, ώστε να είναι σε θέση να παρέχει στο υποκείμενο τα δεδομένα του σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα δια λειτουργικό μορφότυπο, δωρεάν και μέσα σε προθεσμία ενός μήνα.

5) Έλεγχος αν έχουν **υιοθετηθεί τα κατάλληλα οργανωτικά και τεχνικά μέτρα** προκειμένου η επιχείρηση να μπορεί αμέσως και ευχερώς να ανταποκρίνεται σε αιτήματα των υποκειμένων των δεδομένων για πρόσβαση σ' αυτά, ιδίως μάλιστα αν αναμένονται πολλά τέτοια αιτήματα. Εφιστάται η προσοχή στην άσκηση του δικαιώματος πρόσβασης του υποκειμένου διότι στις περισσότερες περιπτώσεις το δικαίωμα πρόσβασης παρέχεται δωρεάν, ενώ η προθεσμία απάντησης είναι μόνο ένας μήνας. Σε περίπτωση άρνησης ικανοποίησης του δικαιώματος πρόσβασης ο υπεύθυνος επεξεργασίας οφείλει να εξηγήσει στο υποκείμενο των δεδομένων χωρίς

αναίτια καθυστέρηση και το αργότερο σε έναν μήνα το λόγο άρνησης, και ταυτόχρονα να ενημερώσει το υποκείμενο για το δικαίωμά του να υποβάλει καταγγελία στην αρμόδια εποπτική αρχή και να προσφύγει δικαστικά κατά του υπευθύνου επεξεργασίας. Στο μέτρο του δυνατού ή του επιθυμητού, αποτελεί "καλή πρακτική" η εγκατάσταση συστήματος που επιτρέπει την επιγραμμική (online) πρόσβαση του υποκειμένου στα προσωπικά του δεδομένα.

6) **Αναθεώρηση της πολιτικής της επιχείρησης αναφορικά με τη λήψη της συγκατάθεσης** ώστε να είναι σύμφωνη προς τις επιταγές του Κανονισμού. Η συγκατάθεση καθίσταται πλέον ρητή, το λεγόμενο opt-in. Οι οργανισμοί θα πρέπει να ελέγξουν αν η πληροφόρηση που παρέχεται σε πολίτες, πελάτες ή εταίρους της επιχείρησης, μέσω εντύπων ή μέσω της ιστοσελίδας της, χρειάζεται να διαφοροποιηθεί και να προσαρμοστεί ανάλογα. Επιπλέον, αν η επιχείρηση έχει Πολιτική Προστασίας της Ιδιωτικής Ζωής, πρέπει να ελέγξει ποιες πτυχές της χρήζουν εκσυγχρονισμού σε συμμόρφωση με τον Κανονισμό. Με άλλα λόγια, η δήλωση συγκατάθεσης δεν συνάγεται από την αδράνεια ή τη σιωπή του υποκειμένου ή τις προεπιλογές (πχ. προσυμπληρωμένα τετραγωνίδια) του υπευθύνου επεξεργασίας.

Επιπλέον πρέπει:

- Το αίτημα για συγκατάθεση του υποκειμένου να τίθεται κατά τρόπο σαφώς διακριτό από άλλα θέματα,
- Η παροχή της συγκατάθεσης να είναι χωριστή από άλλους όρους και προϋποθέσεις,
- Αν η επεξεργασία αφορά πολλαπλούς σκοπούς, τότε να λαμβάνεται συγκατάθεση για όλους τους σκοπούς,
- Η ανάκληση της συγκατάθεσης να μπορεί να γίνεται ευχερώς.

7) **Έλεγχος αν ήδη υφίστανται ή πρέπει να υιοθετηθούν κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων** καθώς και κατάλληλες διαδικασίες για τον εντοπισμό και διερεύνηση των περιπτώσεων παραβίασης προσωπικών δεδομένων και τη γνωστοποίησή τους, ανάλογα με την περίπτωση παραβίασης, στην αρμόδια εποπτική αρχή ή και στο υποκείμενο των δεδομένων. Η επιχείρηση πρέπει να εξασφαλίσει ότι διαθέτει κατάλληλα και εκσυγχρονισμένα τεχνικά και διαδικαστικά μέτρα ασφαλείας και ότι εφαρμόζει τις

αναγκαίες πολιτικές για την προστασία των πληροφοριών που χειρίζεται και τα οποία ανταποκρίνονται στις απαιτήσεις του Κανονισμού.

8) **Σχεδιασμός προϊόντων και υπηρεσιών λαμβάνοντας υπόψιν την προστασία της ιδιωτικότητας εξ ορισμού.** Τέτοιες περιπτώσεις έχουν να κάνουν με την ελαχιστοποίηση των υπό επεξεργασία δεδομένων ως προς τον όγκο τους καθώς και ως προς την ένταση και έκταση της επεξεργασίας και τη διάρκεια τήρησης αυτών, καθώς και με την παροχή στο χρήστη της δυνατότητας ο ίδιος ενεργά να προσδιορίζει την «ορατότητα» του προφίλ του. Επίσης θα πρέπει να υιοθετηθεί και η προστασία εκ σχεδίου και δια σχεδίου, δηλαδή να υπάρχει διαφάνεια όσον αφορά την επεξεργασία, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία των δεδομένων του και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας, καθώς και να επιτυγχάνεται «ψευδωνυμοποίηση» το συντομότερο δυνατόν.

Αξίζει να σημειωθεί πως η λήψη μέτρων προστασίας εκ σχεδίου και δια σχεδιασμού θα πρέπει να γίνεται λαμβάνοντας υπόψη και το κόστος εφαρμογής των μέτρων αυτών καθώς και την πιθανότητα και σοβαρότητα των κινδύνων που μπορεί να προκύψουν (risk assessment). Όπου απαιτείται από τον Κανονισμό, η επιχείρηση οφείλει να προχωρεί σε εκπόνηση εκτίμησης αντικτύπου στην προστασία των προσωπικών δεδομένων, τη γνωστή πλέον Data Protection ImpactAssessement (DPIA). Επομένως κάθε επιχείρηση οφείλει να διερευνήσει:

- Αν της επιβάλλεται από τον Κανονισμό να εκπονήσει DPIA (πχ. περιπτώσεις επεξεργασιών υψηλού κινδύνου),
- Ποιος θα τη διενεργήσει και ποιοι ακόμη χρειάζεται να εμπλακούν (πχ. υπεύθυνος επεξεργασίας, χρήστες του συστήματος, ειδικοί νομικοί και πληροφορικοί),
- Ποια θα είναι η μεθοδολογία και τα τεχνικά πρότυπα (πχ. ISOS) που θα ακολουθηθούν.

Μετά την εκπόνηση της DPIA η επιχείρηση συμμορφώνεται προς τις συστάσεις της και εφαρμόζει τα μέτρα προστασίας προσωπικών δεδομένων που προτείνει.

Υπογραμμίζεται ότι σε κάθε περίπτωση και ανεξάρτητα από το αν η εκπόνηση DPIA είναι υποχρεωτική ή όχι, κάθε επιχείρηση είναι υποχρεωμένη να καταρτίσει και να υλοποιήσει σχέδιο ενεργειών συμμόρφωσης προς τον Κανονισμό, στο μέτρο που ο Κανονισμός την αφορά.

9) **Ορισμός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer)** στις περιπτώσεις που επιβάλλεται από τον Κανονισμό[13]. Σημειώνεται ότι ο DPO μπορεί να είναι και υπάλληλος του οργανισμού και εξωτερικός συνεργάτης με σύμβαση παροχής υπηρεσιών. Ακόμη ανεξάρτητα αν ο διορισμός DPO είναι υποχρεωτικός ή προαιρετικός, η επιχείρηση οφείλει να ορίσει φυσικό πρόσωπο ή ομάδα προσώπων που να είναι αρμόδια για τη συμμόρφωση με τον Κανονισμό και να ενσωματώσει αυτή τη νέα αρμοδιότητα στη δομή και λειτουργία της.

10) Αν η επιχείρηση δραστηριοποιείται σε περισσότερα από ένα κράτη μέλη της Ευρωπαϊκής Ένωσης, υποχρεούται να **αποφασίσει και να καταγράψει ποια είναι η επικεφαλής εποπτική της αρχή**. Για τον καθορισμό της επικεφαλής εποπτικής αρχής το κριτήριο είναι πού βρίσκεται η κύρια ή η μόνη εγκατάσταση του υπευθύνου επεξεργασίας. Αν μια επιχείρηση δεν είναι σίγουρη για το πού βρίσκεται η κύρια εγκατάστασή της, τότε ενδείκνυται μέσω χαρτογράφησης να εντοπίσει τη χώρα όπου λαμβάνονται οι σημαντικότερες αποφάσεις αναφορικά με τις πράξεις επεξεργασίας προσωπικών δεδομένων ώστε βάσει αυτού του κριτηρίου να καθοριστεί η κύρια εγκατάστασή της.

Ιδιαίτερη σημασία έχει ο σωστός καθορισμός της επικεφαλής εποπτεύουσας Αρχής όταν η επιχείρηση προβαίνει σε διασυνοριακή επεξεργασία προσωπικών δεδομένων πχ. διαβιβάσεις δεδομένων σε περισσότερες από μία χώρες της ΕΕ.

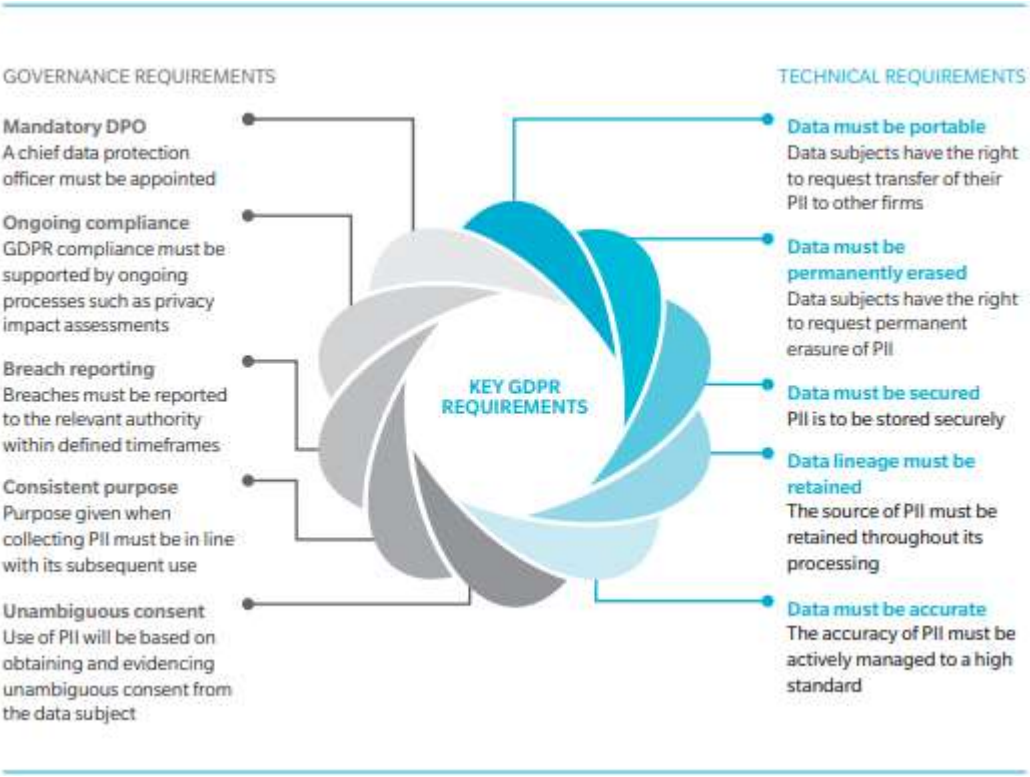
11) Ιδιαίτερη προσοχή στις σχετικές πρόνοιες του Κανονισμού για την **επεξεργασία «ευαίσθητων» δεδομένων**, σε περίπτωση που οι δραστηριότητες του οργανισμού βασίζονται στη συγκατάθεση και να μεριμνήσουν για την ενσωμάτωση δικλείδων ασφαλείας. Ιδιαίτερα, για υπηρεσίες της κοινωνίας των πληροφοριών απευθείας σε παιδιά, θα πρέπει να λαμβάνεται η συγκατάθεση του προσώπου που έχει τη γονική μέριμνα του παιδιού.

12) Ύπαρξη **πλάνου αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων.**

13) Ο οργανισμός θα πρέπει να εξασφαλίζει ότι κάθε δραστηριότητα της επιχείρησης υπακούει **στις προϋποθέσεις για νόμιμη επεξεργασία που καθορίζει ο Κανονισμός,** καθώς και να είναι σε θέση να δικαιολογήσει, εφόσον χρειαστεί, τη νομική βάση στην οποία βασίζεται η κάθε δραστηριότητα της.

[13] Βλ. Κεφάλαιο 4 «Υποχρεωτικός Ορισμός Υπευθύνου Προστασίας Προσωπικών Δεδομένων».

Άλλωστε η επιβολή προστίμου ελλοχεύει ακριβώς, στις περιπτώσεις παραβίασης προσωπικών δεδομένων που ο υπεύθυνος επεξεργασίας ήταν υποχρεωμένος να ανακοινώσει στο υποκείμενο ή στην αρμόδια εποπτική αρχή και παραταύτα παρέμεινε αδρανής. Επομένως, κάθε επιχείρηση οφείλει να καταρτίσει εκ των προτέρων σχέδιο αντιμετώπισης περιστατικών παραβίασης προσωπικών δεδομένων.



Εικόνα 6: Επισκόπηση των βασικών απαιτήσεων GDPR Πηγή: (Wyman , Ivell , Wilkinson , & Helps , 2017)

5.3 Μεθοδολογία Συμμόρφωσης με τον GDPR

Ο κάθε οργανισμός, ιδιωτικός ή δημόσιος, αφού ακολουθήσει τα βήματα προετοιμασίας που αναλύθηκαν προηγουμένως, καλείται να εφαρμόσει την κατάλληλη στρατηγική και μεθοδολογία προκειμένου να προβεί στην συμμόρφωση με τον νέο Κανονισμό GDPR.

Εξ' αρχής, από όταν έγινε γνωστή η υποχρεωτική εφαρμογή του νόμου σε όλα τα κράτη μέλη της ΕΕ, οι αρμόδιες εποπτικές Αρχές Προστασίας Δεδομένων της ΕΕ, δημοσίευσαν μεθοδολογίες και εργαλεία για τις επιχειρήσεις, προκειμένου να διευκολύνουν την ομαλή μετάβασή τους στον νέο κόσμο του GDPR.

Οι μεθοδολογίες αυτές συνοψίζονται στα παρακάτω στάδια (Lambrinoudakis, 2018):

Στάδιο 1: Υποχρεωτικός Διορισμός ενός Υπευθύνου Προστασίας Δεδομένων «DPO».

Ο Κανονισμός, αναφέρει ρητά και υποχρεώνει τις επιχειρήσεις και τους οργανισμούς, που υπόκεινται στις διατάξεις του GDPR να διορίσουν έναν «ηγέτη» στην πιλοτική διακυβέρνηση της προστασίας των δεδομένων εντός της δομής τους, ο οποίος θα εκτελεί εσωτερικά ενημερωτικές, συμβουλευτικές και ελεγκτικές εργασίες. Οι εποπτικές Αρχές Προστασίας Δεδομένων της ΕΕ, συμβούλευσαν τις οντότητες να προβούν νωρίτερα, πριν τις 25 Μαΐου 2018, ημερομηνία καθολικής και υποχρεωτικής εφαρμογής του Νόμου, σε διορισμό Υπευθύνου Προστασίας Προσωπικών Δεδομένων, ώστε να οργανωθούν καλύτερα και να είναι ένα στάδιο μπροστά στο να συμμορφωθούν με τον επερχόμενο Κανονισμό. Ο ορισμός Υπευθύνου Προστασίας δεν είναι πάντοτε υποχρεωτικός. Εξαρτάται από το μέγεθος της εταιρείας, τον τύπο και τον αριθμό των δεδομένων που συλλέγονται, αν η επεξεργασία είναι η κύρια επιχειρηματική δραστηριότητα και αν πραγματοποιείται επεξεργασία δεδομένων σε μεγάλη κλίμακα. Ωστόσο, ο διορισμός ενός DPO ενδείκνυται για τη διασφάλιση της συμμόρφωσης με τον GDPR, ενώ θα πρέπει να πρόκειται για ένα άτομο κατάλληλα καταρτισμένο και προσεκτικά επιλεγμένο ώστε να είναι σε θέση να διεκπεραιώσει τις υποχρεώσεις του, δίχως σύγκρουση συμφερόντων. 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 στάδιο.

Στάδιο 2: Έλεγχος, εντοπισμός, κατάταξη και χαρτογράφηση δεδομένων

Οι οικονομικές οντότητες θα πρέπει να προβούν σε ένα είδος εσωτερικού ελέγχου των λειτουργιών τους. Θα πρέπει να εντοπίσουν και να αναγνωρίσουν αν τηρούν σε οποιαδήποτε μορφή ηλεκτρονική ή μη αρχεία με δεδομένα προσωπικού χαρακτήρα και να προσδιορίσουν λεπτομερώς τις δραστηριότητές τους που υπόκεινται σε επεξεργασία δεδομένων. Επιπλέον θα πρέπει να συλλέξουν και πληροφορίες σχετικά με την φύση των δεδομένων, την κατηγορία στην οποία ανήκουν, τον σκοπό που εξυπηρετεί η συλλογή τους, τον χρόνο και τα μέσα αποθήκευσής τους. Αυτό, μπορούν να το πράξουν με την χρήση ερωτηματολογίων και την πραγματοποίηση συνεντεύξεων ανά Διεύθυνση, προκειμένου να γίνει πλήρης

καταγραφή / αποτύπωση της υφιστάμενης κατάστασης της επιχείρησης και τη διατήρηση ενός μητρώου δραστηριοτήτων επεξεργασίας δεδομένων (κυρίως οι επιχειρήσεις άνω των 250 ατόμων). Επισημαίνεται, ότι στο πλαίσιο του GDPR, οι οργανισμοί θα πρέπει να διατηρούν πλήρη εσωτερική τεκμηρίωση των δραστηριοτήτων επεξεργασίας των δεδομένων τους, κατά προτίμηση διατηρώντας ένα πρότυπο μητρώο δεδομένων.

Για να συνεχίσουν οι οργανισμοί στο επόμενο στάδιο της μεθοδολογίας συμμόρφωσης με τον GDPR, θα πρέπει να ελέγξουν αν:

- ✓ Η οργανωτική τους δομή περιλαμβάνει όλες τις κατάλληλες υπηρεσίες και οντότητες που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.
- ✓ Έχουν καταρτίσει κατάλογο των δραστηριοτήτων επεξεργασίας δεδομένων τους κατά κύριο σκοπό και τους τύπους επεξεργασμένων δεδομένων προσωπικού χαρακτήρα.
- ✓ Έχουν θεσπίσει και εντοπίσει τους υπευθύνους συλλογής και επεξεργασίας δεδομένων που συμμετέχουν σε κάθε δραστηριότητα επεξεργασίας δεδομένων.
- ✓ Γνωρίζουν που μεταφέρονται τα δεδομένα, σε ποιον, πού φιλοξενούνται και για πόσο χρονικό διάστημα διατηρούνται.

Πρόκειται για ένα πολύ σημαντικό στάδιο της διαδικασίας συμμόρφωσης, το οποίο στην ουσία «ξεκλειδώνει» τα επόμενα βήματα.

Στάδιο 3: Εντοπισμός κινδύνων-ελλείψεων και προτεραιότητα στις ενέργειες συμμόρφωσης

Αξιοποιώντας την πλήρη γνώση της ροής των προσωπικών δεδομένων (3ο βήμα), η επιχείρηση οφείλει να καταγράψει τους πιθανούς κινδύνους και τις ελλείψεις που - ενδεχομένως - εντοπίστηκαν (να πραγματοποιήσει δηλαδή την επονομαζόμενη "gap analysis"). Έτσι καταρτίζεται ένας πίνακας ο οποίος περιέχει τις δραστηριότητες που εντοπίστηκαν με ελλείψεις, την προτεραιοποίησή τους με βάση τον κίνδυνο που ενέχουν και τις προτεινόμενες ενέργειες για την αντιμετώπισή τους. Παραδείγματα σχετικών «κενών» είναι: πολύ μεγάλη περίοδος διατήρησης των δεδομένων άνευ λόγου, διατήρηση των ίδιων δεδομένων σε περισσότερα του ενός σημεία και ανεμπόδιστη πρόσβαση σε δεδομένα από όλα τα στελέχη ενώ δεν χρειάζεται. Ακόμη θα πρέπει να γίνει προσδιορισμός και ιεράρχηση των ενεργειών που πρέπει να εφαρμοστούν για να συμμορφωθεί η εκάστοτε επιχείρηση ή οργανισμός με τις

τρέχουσες και μελλοντικές υποχρεώσεις προστασίας προσωπικών δεδομένων, για κάθε δραστηριότητα επεξεργασίας δεδομένων. Πρέπει να σημειωθεί, πως η ιεράρχηση αυτή, πρέπει να πραγματοποιηθεί με γνώμονα τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ενώ θα πρέπει να περιλαμβάνουν τουλάχιστον:

- Τον προσδιορισμό της νομικής βάσης για την επεξεργασία δεδομένων
- Τη διαβεβαίωση και τη διασφάλιση ότι συλλέγονται και επεξεργάζονται μόνο προσωπικά δεδομένα που είναι απολύτως απαραίτητα.
- Γίνεται επανεξέταση των τωρινών ειδοποιήσεων απορρήτου, ώστε να συμμορφωθεί ο οργανισμός με τις απαιτήσεις που ορίζει ο Κανονισμός.
- Την εξασφάλιση ότι όλοι οι υπεύθυνοι και επεξεργαστές δεδομένων είναι γνώστες όλων των διατάξεων και άρθρων που υπάρχουν στο νέο Κανονισμό
- Τον καθορισμό διαδικασίας για τη διεκπεραίωση των αιτημάτων των υποκειμένων των δεδομένων για την άσκηση των δικαιωμάτων προστασίας των δεδομένων τους.
- Τέλος, την επαλήθευση των μέτρων ασφαλείας προσωπικών δεδομένων που εφαρμόζονται.

Ωστόσο πρέπει να σημειωθεί πως αν οι οντότητες, δεν έχουν εντοπίσει εκείνες τις δραστηριότητες που σχετίζονται με την επεξεργασία δεδομένων, τότε δεν μπορούν να ολοκληρώσουν το τρίτο στάδιο και να μεταβούν στο επόμενο.

Στάδιο 4: <u>Διαχείριση και αντιμετώπιση κινδύνων (DPIA)</u>

Εάν, κατά το προηγούμενο στάδιο, οι οργανισμοί έχουν εντοπίσει δραστηριότητες επεξεργασίας δεδομένων που ενδέχεται να ενέχουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, θα πρέπει να διενεργήσουν εκτίμηση επιπτώσεων στην ιδιωτική ζωή (DPIA) για καθεμία από αυτές τις δραστηριότητες επεξεργασίας δεδομένων. Πρόκειται για υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, προαιρετικό για τις υπόλοιπες. Η εκπόνηση της εκτίμησης αντικτύπου εξ ορισμού προηγείται της επεξεργασίας των δεδομένων και περιλαμβάνει ανάλυση για τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα. Καταλήγει σε κατηγοριοποίηση των δραστηριοτήτων

επεξεργασίας σε υψηλού, μεσαίου και χαμηλού κινδύνου και σε επανεξέταση των απαιτούμενων διαδικασιών σε κάθε περίπτωση.

Το τέταρτο στάδιο θα ολοκληρωθεί μόλις οι οργανισμοί εφαρμόσουν μέτρα για την αντιμετώπιση των κυριότερων κινδύνων και απειλών για την ιδιωτική ζωή των προσώπων στα οποία αναφέρονται τα δεδομένα.

Στάδιο 5: Οργάνωση των εσωτερικών διαδικασιών

Η έννοια του ελέγχου των εσωτερικών διαδικασιών μιας οικονομικής οντότητας, θα πρέπει να αποτελεί σημαντικό και αναπόσπαστο κομμάτι της, ώστε να εξασφαλίζεται η εύρυθμη λειτουργία της και η μακροημέρευσή της. Συνεπώς και για την επιτυχή εφαρμογή και συμμόρφωση με τον νέο Κανονισμό, η έννοια του εσωτερικού ελέγχου αποτελεί σημαντικό παράγοντα ώστε να αποφευχθεί η επιβολή προστίμων και κυρώσεων. Με βάση τα συμπεράσματα των βημάτων 3 και 4, η επιχείρηση προβαίνει σε αναθεώρηση των πολιτικών και των διαδικασιών τήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα, οι οργανισμοί θα πρέπει να επανασχεδιάσουν και να εφαρμόσουν εσωτερικές διαδικασίες για να εγγυώνται την προστασία των δεδομένων τους ανά πάσα στιγμή, λαμβάνοντας υπόψη όλα τα συμβάντα που μπορεί να προκύψουν κατά τη διάρκεια μιας δραστηριότητας επεξεργασίας δεδομένων (όπως παραβίαση της ασφάλειας των δεδομένων, διαχείριση των αιτημάτων των υποκειμένων των δεδομένων, φύση των δεδομένων που συλλέγονται, αλλαγή του προσωπικού κ.λπ.).

Συγκεκριμένα θα πρέπει να ακολουθήσει τις εξής ενέργειες:

- ✓ Ανάπτυξη στρατηγικών διαχείρισης των πιθανών απειλών σε συνεργασία με τους αρμόδιους υπευθύνους και τις αρμόδιες Αρχές Προστασίας Δεδομένων κατά το σχεδιασμό μιας εφαρμογής ή μιας δραστηριότητας επεξεργασίας δεδομένων.
- ✓ Εφαρμογή τεχνικών μέτρων που να διασφαλίζουν την ακεραιότητα των δεδομένων, όπως είναι η «ψευδωνυμοποίηση και κρυπτογράφηση» ή μεθόδων περισσότερο φιλικών για το χρήστη, όπως η «προστασία κατά το σχεδιασμό εξ' ορισμού».
- ✓ Αύξηση της ευαισθητοποίησης των εργαζομένων και διασφάλιση της κλιμάκωσης των πληροφοριών στους αρμόδιους υπαλλήλους ή διευθυντές, ιδίως με την ανάπτυξη σχεδίου κατάρτισης και επικοινωνιών.

✓ Διαρκής εκπαίδευση του προσωπικού στο χειρισμό των καταγγελιών των υποκειμένων των δεδομένων, καθώς και παροχή σεμιναρίων για καλύτερη γνώση του τωρινού Κανονισμού αλλά και μελλοντικών που αφορούν τα προσωπικά δεδομένα.

✓ Πρόβλεψη των παραβιάσεων ασφαλείας των δεδομένων, διασφαλίζοντας ότι σε ορισμένες περιπτώσεις η παραβίαση θα πρέπει να κοινοποιείται στην Αρχή Προστασίας Δεδομένων εντός 72 ωρών και χωρίς αδικαιολόγητη καθυστέρηση στα θιγόμενα πρόσωπα που επηρεάζονται.

Στάδιο 6: Αξιοποίηση των εργαλείων πληροφορικής

Κάθε επιχείρηση ανάλογα με τη φύση των εργασιών της, τα μεγέθη και τις δυνατότητές της, οφείλει να αξιοποιήσει κάποια από τα εργαλεία πληροφορικής που ενισχύουν την ασφάλεια των συστημάτων. Ενδεικτικά παραδείγματα αποτελούν: εργαλεία που με αυτοματοποιημένο τρόπο χαρτογραφούν τα δεδομένα (3ο βήμα), εργαλεία που αξιολογούν την αποτελεσματικότητα των πολιτικών και διαδικασιών που έχουν αναπτυχθεί και εργαλεία που βοηθούν στην αποτροπή ή τον εντοπισμό των αποπειρών παραβίασης δεδομένων. Επιπλέον, η κρυπτογράφηση και η ψευδωνυμοποίηση αποτελούν δύο εκ των απλούστερων τεχνικών μέτρων προστασίας.

Στάδιο 7: Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκειμένου

Πρόκειται για δύο υποχρεωτικές διαδικασίες για κάθε επιχείρηση. Η πρώτη αφορά στη διαδικασία γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική Αρχή, εντός μόλις 72 ωρών από τη στιγμή που η επιχείρηση αποκτά γνώση του γεγονότος. Το σύντομο χρονικό διάστημα που προβλέπεται είναι προφανές ότι αυξάνει το βαθμό δυσκολίας. Η δεύτερη αφορά στη διαδικασία άμεσης ανακοίνωσης της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν υπάρχει ενδεχόμενο να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες του. Ο επικοινωνιακός χειρισμός σε αυτήν την περίπτωση είναι κρίσιμης σημασίας και μπορεί να κάνει τη διαφορά όσον αφορά στη φήμη της επιχείρησης.

Στάδιο 8: Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών

Πρόκειται για το τελευταίο χρονικά στάδιο. Αναφέρεται σε δοκιμαστικούς ελέγχους επί των συστημάτων και διαδικασιών που έχει αναπτύξει η επιχείρηση στα προηγούμενα βήματα, ώστε να αποδειχθεί ότι μετά την 25η Μαΐου 2018 οι ενέργειες συμμόρφωσης δούλεψαν αποτελεσματικά στην πράξη. Ενδεχομένως να οδηγήσει σε ανάγκη υλοποίησης διορθωτικών παρεμβάσεων

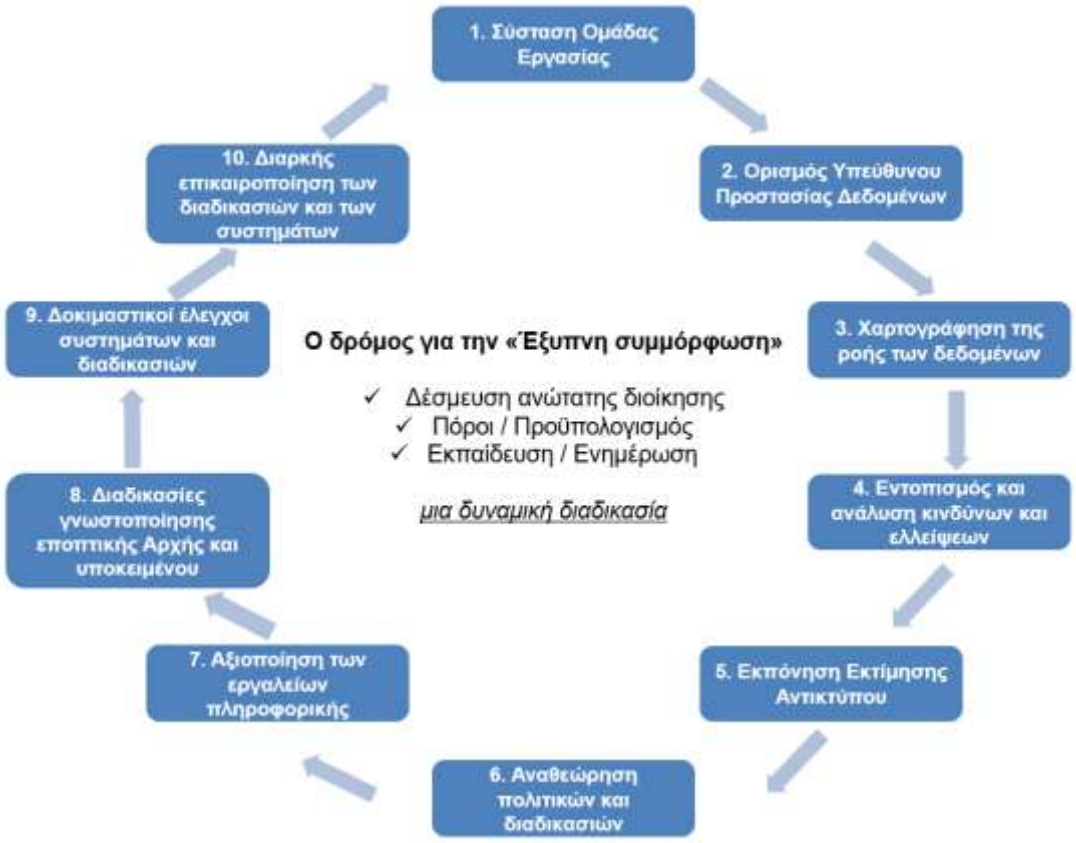
Στάδιο 9: Διατήρηση της τεκμηρίωση και απόδειξης σχετικά με τα μέτρα συμμόρφωσης

Οι οργανισμοί, είναι επιφορτισμένοι και με την υποχρέωση να αποδεικνύουν οι ίδιοι την συμμόρφωσή τους με τις απαιτήσεις του νέου Κανονισμού. Αυτό επιτυγχάνεται με την συγκέντρωση όλων των απαραίτητων εγγράφων και ενεργειών που εκπονήθηκαν σε κάθε στάδιο. Τα έγγραφα και οι ενέργειες αυτές, θα πρέπει να επανεξετάζονται και να ενημερώνονται τακτικά, ώστε να διασφαλίζεται η συνεχής και επιτυχής προστασία των προσωπικών δεδομένων.

Για να γίνει πιο σαφές αυτό, οι οργανισμοί θα πρέπει να προβούν σε αυτή την τεκμηρίωση με την χρήση:

- ✓ Του μητρώου δραστηριοτήτων επεξεργασίας δεδομένων (για τους υπευθύνους επεξεργασίας δεδομένων) ή τις κατηγορίες δραστηριοτήτων επεξεργασίας δεδομένων (για τους εκτελούντες την επεξεργασία των δεδομένων).
- ✓ Της εκτίμηση των επιπτώσεων (DPIA) για επεξεργασία δεδομένων υψηλού κινδύνου.
- ✓ Των μηχανισμών μεταφοράς δεδομένων (π.χ. πρότυπα Ευρωπαϊκής Ένωσης, δεσμευτικοί εταιρικοί κανόνες και πιστοποιήσεις, κ.λπ.).
- ✓ Ειδοποιήσεις απορρήτου.
- ✓ Εντύπων συναίνεσης, καθώς και αποδεικτικά στοιχεία ότι τα υποκείμενα των δεδομένων έχουν δώσει τη συγκατάθεσή τους όταν η συναίνεση αποτελεί τη νομική βάση για την επεξεργασία δεδομένων.
- ✓ Των διαδικασιών που εφαρμόζονται για την άσκηση των δικαιωμάτων προστασίας δεδομένων των υποκειμένων των δεδομένων.
- ✓ Συμβάσεων με τους αρμόδιους παρόχους, επεξεργαστές και υπευθύνους δεδομένων.
- ✓ Των Εσωτερικών διαδικασιών που εφαρμόζονται σε περίπτωση παραβίασης των δεδομένων.

Ολοκλήρωση του τελευταίου σταδίου, θα πραγματοποιηθεί όταν ο έλεγχος αποδείξει τη συμμόρφωση με όλες τις υποχρεώσεις που ορίζει ο GDPR,οπότε και η οντότητα δημόσια η ιδιωτική θα έχει ενταχθεί και επίσημα μέσω της συμμόρφωσής της στον νέο Κανονισμό.



Εικόνα 7 : Οδικός Χάρτης Συμμόρφωσης με τον GDPR. Πηγή: (Ομάδα εργασίας του ΣΕΒ για τα προσωπικά δεδομένα, Οκτώβριος 2018)

5.4 Εκπαίδευση του ανθρώπινου δυναμικού

Η σωστή εκπαίδευση και κατάρτιση του ανθρώπινου δυναμικού μιας οικονομικής οντότητας, αποτελούσε και συνεχίζει να αποτελεί τον σημαντικότερο παράγοντα εξασφάλισης της εύρυθμης λειτουργίας της, καθώς και της μακροημέρευσής της. Όταν υπάλληλοι εργάζονται σε τομείς που δεν έχουν εκπαιδευθεί ή καταρτιστεί, τότε υπάρχει μεγάλος κίνδυνος ανθρώπινου λάθους, που θα ζημιώσει την οικονομική οντότητα είτε είναι ιδιωτική, είτε δημόσια.

Κάτι αντίστοιχο είναι πολύ πιθανόν να συμβεί και με την εφαρμογή του νέου Κανονισμού σχετικά με την Προστασία των Προσωπικών Δεδομένων. Η ύπαρξη

στον Κανονισμό υψηλών προστίμων σε περίπτωση λάθους ή μη σωστής συμμόρφωσης με αυτόν, καθιστούν ακόμη πιο απαραίτητη και επιτακτική την εκπαίδευση του προσωπικού. Οι οντότητες θα πρέπει να αποδείξουν τη συμμόρφωσή τους με τον Κανονισμό και ως εκ τούτου η κατάρτιση του προσωπικού και η καταγραφή και παρακολούθηση της εκπαίδευσης τους θα είναι μια βασική πτυχή της απόδειξης ότι ο οργανισμός συμμορφώνεται με τον GDPR. Υπάρχουν τεχνικές ή συμβουλές που μπορούν να ακολουθήσουν οι οργανισμοί, ούτως ώστε να επιτύχουν την καλύτερη και αποδοτικότερη εκπαίδευση των υπαλλήλων τους, όσον αφορά τον GDPR; Παρακάτω ακολουθούν κάποιες συμβουλές για την καλύτερη εκπαίδευση του προσωπικού:

- ✓ **Κατανόηση του Γενικού Κανονισμού Προστασίας Δεδομένων**

Οι εργαζόμενοι πρέπει να κατανοήσουν τα όσα ορίζονται στον Κανονισμό, τους οικονομικούς κινδύνους και τους κινδύνους υπόληψης της επιχείρησης, καθώς και τον κίνδυνο ενδεχόμενων πειθαρχικών μέτρων ή ακόμη και της απόλυσης σε περίπτωση υπαιτιότητάς τους για παραβίαση δεδομένων που βλάπτει την επιχείρηση.

Όταν οι κίνδυνοι συσχετίζονται με την ιδέα πίσω από τον GDPR, οι εργαζόμενοι μπορούν ευκολότερα να αρχίσουν να κατανοούν τη σημασία των νόμων περί προστασίας δεδομένων, τους λόγους που υπάρχουν ορισμένες πολιτικές και διαδικασίες και γιατί πρέπει να συμμορφώνονται με αυτές. Αυτό μπορεί να επιτευχθεί μέσω της παροχής στοχοθετημένων πρωτοβουλιών ευαισθητοποίησης του προσωπικού στον τρόπο που αντιμετωπίζουν βασικούς επιχειρηματικούς στόχους.

- ✓ **Συνεχής και εμπεριστατωμένη εκπαίδευση**

Η εκπαίδευση πρέπει να είναι πολύ συγκεκριμένη, έτσι ώστε οι υπάλληλοι να μπορούν να συσχετίζουν τις πολιτικές και τις διαδικασίες που εφαρμόζει ο οργανισμός γύρω από τη συμμόρφωση με τον GDPR στους καθημερινούς τους ρόλους.

Ενδεικτικά, μπορεί να περιλαμβάνει ενημέρωση σχετικά με τη σημασία της υιοθέτησης «ισχυρών» κωδικών πρόσβασης και της συχνής αλλαγής αυτών, μέχρι πρακτικές για την ασφαλή καταστροφή και κρυπτογράφηση δεδομένων και διατήρηση ασφαλών και εμπιστευτικών φακέλων στο χώρο του γραφείου.

- ✓ **Εκπαίδευση ανάλογα με τη θέση και τις αρμοδιότητες στην επιχείρηση**

Ο τρόπος που εκπαιδεύεται το προσωπικό, πρέπει να αντικατοπτρίζει τις αρμοδιότητες και να λαμβάνει υπόψη τις διαφορετικές θέσεις και τους πολλαπλούς ρόλους που υπάρχουν μέσα στον ίδιο οργανισμό..

Συγκεκριμένα, όσοι χειρίζονται χρηματοοικονομικές πληροφορίες, πρέπει να εξασκήσουν τις δεξιότητες που απαιτούνται για την εξασφάλιση δεδομένων πιστωτικών καρτών και όλων των πηγών χρηματοοικονομικών δεδομένων, όπως ακριβώς και οι νοσηλευτές και οι επαγγελματίες του τομέα υγείας πρέπει να προστατεύσουν τις εμπιστευτικές πληροφορίες για την υγεία.

Οι διευθυντές και τα στελέχη πρέπει να κατανοήσουν ότι η αυξημένη πρόσβασή τους στις πληροφορίες, τους καθιστά στόχους

Το προσωπικό πληροφορικής χρειάζεται ειδική εκπαίδευση, όχι μόνο για την προνομιακή πρόσβαση στα δεδομένα αλλά και για το ρόλο που διαδραματίζουν ως πρεσβευτές στην κατανόηση και τη χρήση της τεχνολογίας των πληροφοριών για την προστασία των πληροφοριών.

Με αυτόν το διαχωρισμό, καθίσταται ευκολότερη η εκπαίδευση και ο σχεδιασμός ενός πλάνου που προσαρμόζεται σε όλες τις εργασιακές θέσεις.

- ✓ **Εκπαίδευση με φυσική παρουσία των εργαζομένων**

Ενώ η δια ζώσης ή εξ' αποστάσεως εκπαίδευση είναι μια βιώσιμη επιλογή, τίθεται το ερώτημα σε ποιο βαθμό «απορροφάτε» πλήρως από τους εργαζόμενους και σε ποιο βαθμό οι εργαζόμενοι μπορούν να συνδέσουν τις «εξ' αποστάσεως» αυτές πληροφορίες εκπαίδευσης στους καθημερινούς τους ρόλους.

Συνεπώς, προτείνεται να εκτελούνται εκπαιδευτικές συναντήσεις- σεμινάρια με φυσική παρουσία των ενδιαφερομένων, ώστε να δίνεται η ευκαιρία στους υπαλλήλους να θέτουν συναφείς ερωτήσεις και να επωφελούνται από τον διάλογο που οδηγεί αυτά τα ερωτήματα στη συσχέτισή τους με αυτό που κάνουν σε καθημερινή βάση.

- ✓ **Εκπαίδευση εντοπισμού παραβιάσεων προσωπικών δεδομένων**

Μία από τις νέες πτυχές του GDPR, είναι η υποχρέωση των εργαζομένων να αναφέρουν παραβιάσεις δεδομένων εντός προθεσμίας 72 ωρών στις αρμόδιες εποπτικές αρχές πληροφόρησης, καθώς και να τις γνωστοποιούν στα άτομα που

τέθηκαν τα δεδομένα τους σε κίνδυνο, μια υποχρέωση που μέχρι πρότινος δεν υφίστανται στον ιδιωτικό τουλάχιστον τομέα.

Το προσωπικό συνεπώς, πρέπει να είναι σε θέση να εντοπίσει πότε έχει σημειωθεί πιθανή παραβίαση, πώς αναφέρεται η ύπαρξη πιθανής παραβίασης εσωτερικά, στον Υπεύθυνο Προστασίας Δεδομένων του οργανισμού, και εντός ποιου χρονικού διαστήματος. Δεδομένου ότι οι εργαζόμενοι θα είναι συχνά οι πρώτοι που θα έχουν επίγνωση ότι έχει σημειωθεί παραβίαση, πρέπει να υπάρχει σαφής πολιτική για την αναφορά της πιθανής παραβίασης, ώστε ο οργανισμός να μπορεί να συμμορφωθεί με τις υποχρεώσεις υποβολής εκθέσεων και αναφορών.

Έτσι, εάν η εκπαίδευση σχετίζεται με το τι κάνει μια συγκεκριμένη επιχείρηση στην πράξη, τότε σε καταστάσεις «εκτάκτου κινδύνου» καθίσταται ευκολότερο για τους εργαζομένους να εντοπίσουν και να μεταβιβάσουν στο κατάλληλο άτομο τις πληροφορίες, μειώνοντας σημαντικά τον πιθανό κίνδυνο μη συμμόρφωσης.

✓ **Υιοθέτηση κοινής κουλτούρας για την προστασία των προσωπικών δεδομένων**

Είναι σημαντικό να υπάρχει διαφάνεια και να ενισχύεται η προβολή των προσπαθειών για την προώθηση της προστασίας των πληροφοριών, καθώς είναι ζωτικής σημασίας για την ανάπτυξη μιας κουλτούρας που σέβεται την προστασία της ιδιωτικής ζωής μέσα στον οργανισμό ή την επιχείρηση. Αυτή είναι η ευκαιρία να βεβαιωθεί η επιχείρηση ότι ο κάθε εργαζόμενος κάνει την προστασία, της ιδιωτικής ζωής και των δεδομένων, ευθύνη του.

✓ **Άμεση έναρξη της εκπαίδευσης και διασφάλισης συνέχειάς της**

Δεδομένου ότι δεν υπήρχε περίπτωση παράτασης της περιόδου «χάριτος» για συμμόρφωση με το νέο Κανονισμό, οι οργανισμοί πρέπει να έχουν ήδη εναρμονιστεί πλήρως με τους νέους κανόνες. Έτσι, όσο πιο οργανωμένη και έτοιμη είναι μια επιχείρηση ως προς τη συμμόρφωση με τον GDPR, τόσο μικρότερος είναι ο κίνδυνος παραβιάσεων που συμβαίνουν όταν αρχίσουν να ισχύουν οι κανόνες του GDPR.

Ωστόσο, οι επιχειρήσεις δεν πρέπει να επαναπαύονται απλά στην εκπαίδευση των εργαζομένων τους, αλλά η κατάρτιση αυτή πρέπει να είναι συνεχής και αδιάλειπτη, ώστε να συμπεριληφθούν και τα νέα μέλη του προσωπικού. Επιπλέον, το προσωπικό θα πρέπει να εκπαιδεύεται σε θέματα του GDPR ως μέρος της συνεχούς

εξέλιξής του, ώστε να ενστερνιστεί πλήρως τους νέους κανόνες και να οδηγηθεί πραγματικά στην υιοθέτηση και την εφαρμογή τους. Με αυτό τον τρόπο, οι εργαζόμενοι θα είναι προετοιμασμένοι να χειριστούν και να αποφύγουν τυχόν παραβιάσεις προσωπικών δεδομένων και κατά επέκταση την επιβολή υψηλών προστίμων στην οντότητα στην οποία εργάζονται. .

5.5 Διαμόρφωση ηθικής νοοτροπίας και επικαιροποίηση του GDPR

Μετά τα στάδια εναρμόνισης της οικονομικής οντότητας, με τους κανονισμούς του GDPR και την κατάλληλη εκπαίδευση του ανθρώπινου δυναμικού της, η οντότητα θα πρέπει να διαμορφώσει μια ηθική και ορθή νοοτροπία. Η υιοθέτηση μιας τέτοιας νοοτροπίας θα πρέπει να αποτελεί για την οντότητα ζωτικής σημασίας προτεραιότητα, διότι ειδάλλως η εστιασμένη προσέγγισή της στη συμμόρφωση για την εξάλειψη ανήθικων συμπεριφορών ενδέχεται να ανακόψει τις προσπάθειές της να καινοτομεί και να λαμβάνει τα αναμενόμενα υγιή ρίσκα.

Η συνεχής επένδυση σε εκπαίδευση και επιμόρφωση σε θέματα συμμόρφωσης με τον GDPR, ενθαρρύνει τον υγιή ανταγωνισμό και την εξωστρέφεια των επιχειρήσεων, ευθυγραμμίζει την εταιρική νοοτροπία με αυτή των επιχειρήσεων του εξωτερικού και έχει ως αποτέλεσμα την αδιαπραγμάτευτη ανάπτυξη και εδραίωση της θέσης της επιχείρησης στην αγορά καθώς και τη δημιουργία συνεργασιών εμπιστοσύνης εντός και εκτός Ελλάδος. Το τελευταίο ίσως αποτελεί και το σημαντικότερο όφελος μιας ολοκληρωμένης Στρατηγικής Συμμόρφωσης.

Τόσο η διοίκηση του οργανισμού, όσο και το ανθρώπινο δυναμικό της, θα πρέπει μετά το πέρας της συμμόρφωσης με τον Κανονισμό, να βρίσκονται σε συνεχή εγρήγορση κα να παρακολουθούν γεγονότα γύρω από τον GDPR, καθώς και να επικαιροποιούν τις γνώσεις και τις δεξιότητές τους με νέες, είτε μέσω συμμετοχής και παρακολούθησης επιμορφωτικών σεμιναρίων, είτε μέσω παρακολούθησης εκπαιδευτικών προγραμμάτων.

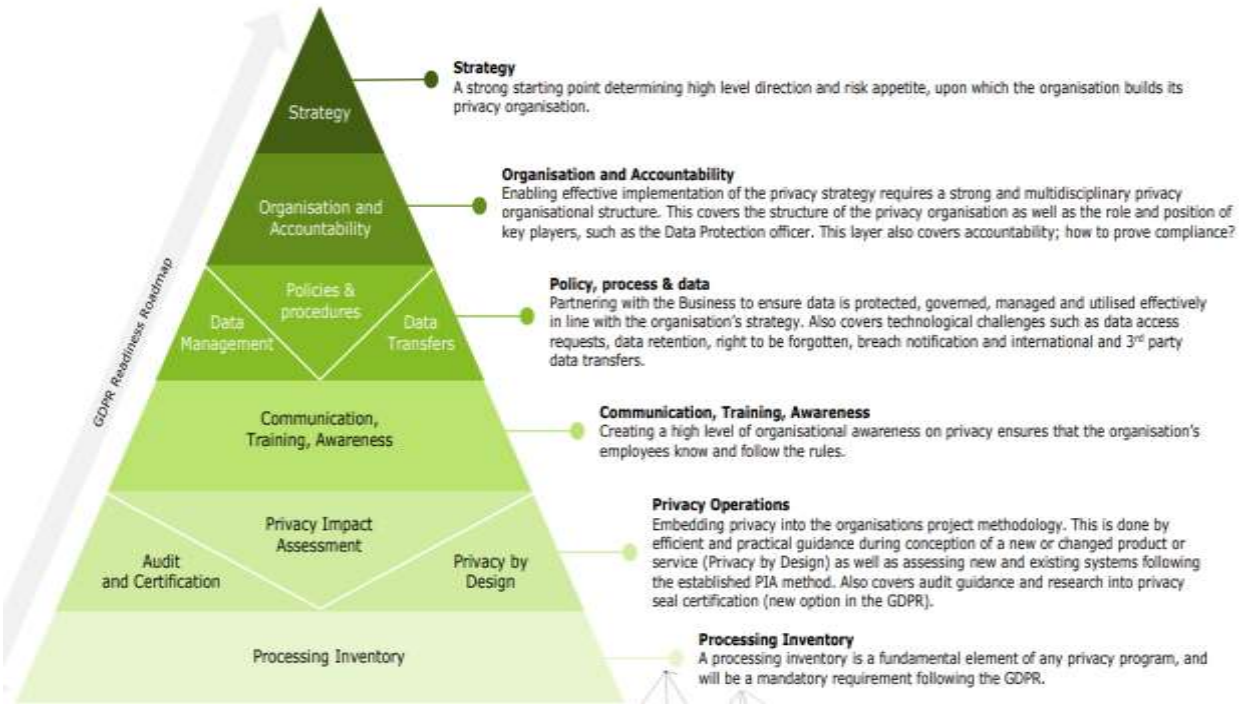
Τέτοια προγράμματα μπορεί να περιλαμβάνουν μελέτες περιπτώσεων (case studies) ή χρήση οδηγών, τα οποία αποτελούν και τα βασικά και μοναδικά εργαλεία των DPOs, για την δημιουργία και μελέτη διάφορων σεναρίων-περιπτώσεων

παραβίασης προσωπικών δεδομένων και άμεση ανταπόκριση σε αυτές, μέσω ήδη προετοιμασμένων σεναρίων-λύσεων.

Η παρακολούθησή τους, θα βοηθήσει τους εργαζόμενους να ακολουθούν αποτελεσματικά τις εξελίξεις και να γίνουν πιο ανταγωνιστικοί στη συνεχώς μεταβαλλόμενη και τεχνολογικά εξελισσόμενη αγορά εργασίας. Επιπλέον, θα αναβαθμίσουν τα ατομικά τους χαρακτηριστικά (γνώσεις, δεξιότητες, συμπεριφορές) προς όφελος της επαγγελματικής τους εξέλιξης, θα μάθουν να διαχειρίζονται τις συνεχείς μεταβολές στον εργασιακό τους χώρο, βελτιώνοντας την ευελιξία και την προσαρμοστικότητα τους σε αυτές, και θα αποκτήσουν όλα τα απαραίτητα εφόδια για να εκτελούν με επιτυχή και παραγωγικό τρόπο την εργασία που τους ανατίθεται, τονώνοντας παράλληλα την απόδοση της επιχείρησης.

Συνεπώς, η συνεχής εκπαίδευση των εργαζομένων και μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης με τον GDPR, είναι ζωτικής σημασίας για την επιχείρηση μιας και μέσω αυτής, δημιουργείται μια ευρύτερη οργανωτική κουλτούρα. Η επιχείρηση αποκτά ανταγωνιστικό πλεονέκτημα, εξελίσσεται, δείχνει τη δυναμική της και ικανοποιεί τους στρατηγικούς της στόχους.

Είναι άλλωστε γνωστό, ότι οι οικονομικές οντότητες δεν είναι εντελώς ενάρετες ούτε όμως και δίχως αξίες. Ο στόχος για αυτές είναι να γίνουν καλύτερες απ’ όσο υπήρξαν και για τους ηγέτες τους να διδάξουν την αρμόζουσα συμπεριφορά με το δικό τους παράδειγμα. Ως εκ τούτου, η πορεία προς την αριστεία, δεν είναι μια πράξη από μόνη της, αλλά μια συνήθεια που επιτυγχάνεται με συνεχή προσπάθεια και θέληση για εξέλιξη και μάθηση.



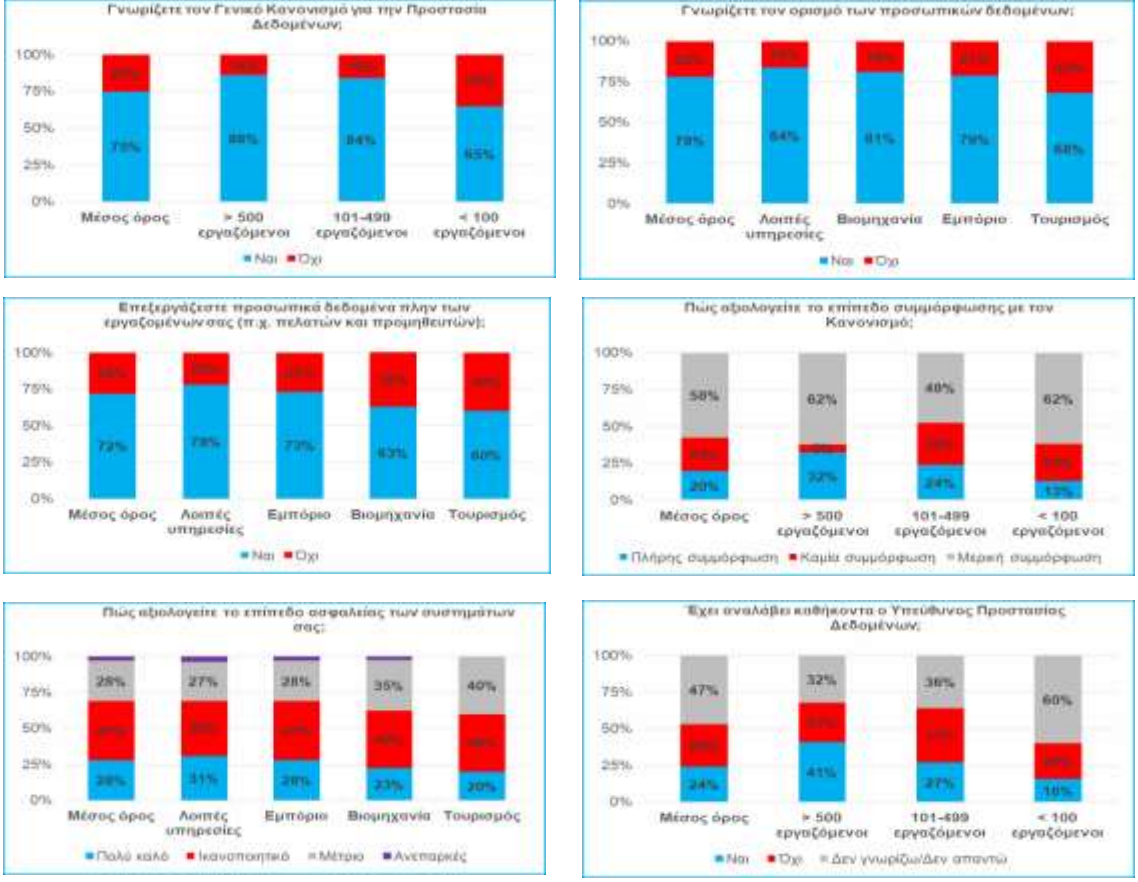
Εικόνα 8: Όλες οι δράσεις που πρέπει να γίνουν για επιτυχή συμμόρφωση με τον GDPR (Πηγή: Deloitte)

5.6 Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στην Ελλάδα

Ο βαθμός ετοιμότητας των ελληνικών επιχειρήσεων για την συμμόρφωση τους με τον GDPR, έχει γίνει αντικείμενο πολλών ερευνών, ακόμα και πριν από την καθολική ισχύ του Κανονισμού, ήτοι τις 25 Μαΐου του 2018. Τα στοιχεία που παρουσιάζονται παρακάτω, προκύπτουν από δύο πρόσφατες έρευνες που δημοσιοποιήθηκαν και αποτυπώνεται με γλαφυρότητα, ότι υπάρχει ακόμη αρκετός δρόμος ακόμα προκειμένου οι ελληνικές επιχειρήσεις να καταφέρουν να συμμορφωθούν στις διατάξεις του Κανονισμού.

5.6.1 Η έρευνα της ICAP

Η έρευνα της ICAP πραγματοποιήθηκε τον Δεκέμβριο 2017, με ηλεκτρονικό ερωτηματολόγιο και το δείγμα ανήλθε σε 210 επιχειρήσεις. Τα συμπεράσματα που προκύπτουν δεν είναι ιδιαίτερα αισιόδοξα όσον αφορά στο βαθμό ετοιμότητας των επιχειρήσεων.



Εικόνα 9: Έρευνα για το επίπεδο συμμόρφωσης των επιχειρήσεων με τον Κανονισμό στην Ελλάδα
Πηγή: ICAP Management Consultants, Φεβρουάριος 2018

Ειδικότερα:

✓ **1 στις 4 επιχειρήσεις δηλώνει ότι δεν γνωρίζει τον νέο Κανονισμό**. Το ποσοστό αυτό αυξάνεται σε 35% για τις επιχειρήσεις με λιγότερο από 100 εργαζομένους.

✓ **Μερίδιο 22% δηλώνει ότι, ακόμα (Δεκέμβριος 2017), δεν γνωρίζει τον ορισμό των προσωπικών δεδομένων**. Το ποσοστό αυτό αυξάνεται σε 32% για τις επιχειρήσεις που δραστηριοποιούνται στον κλάδο του Τουρισμού.

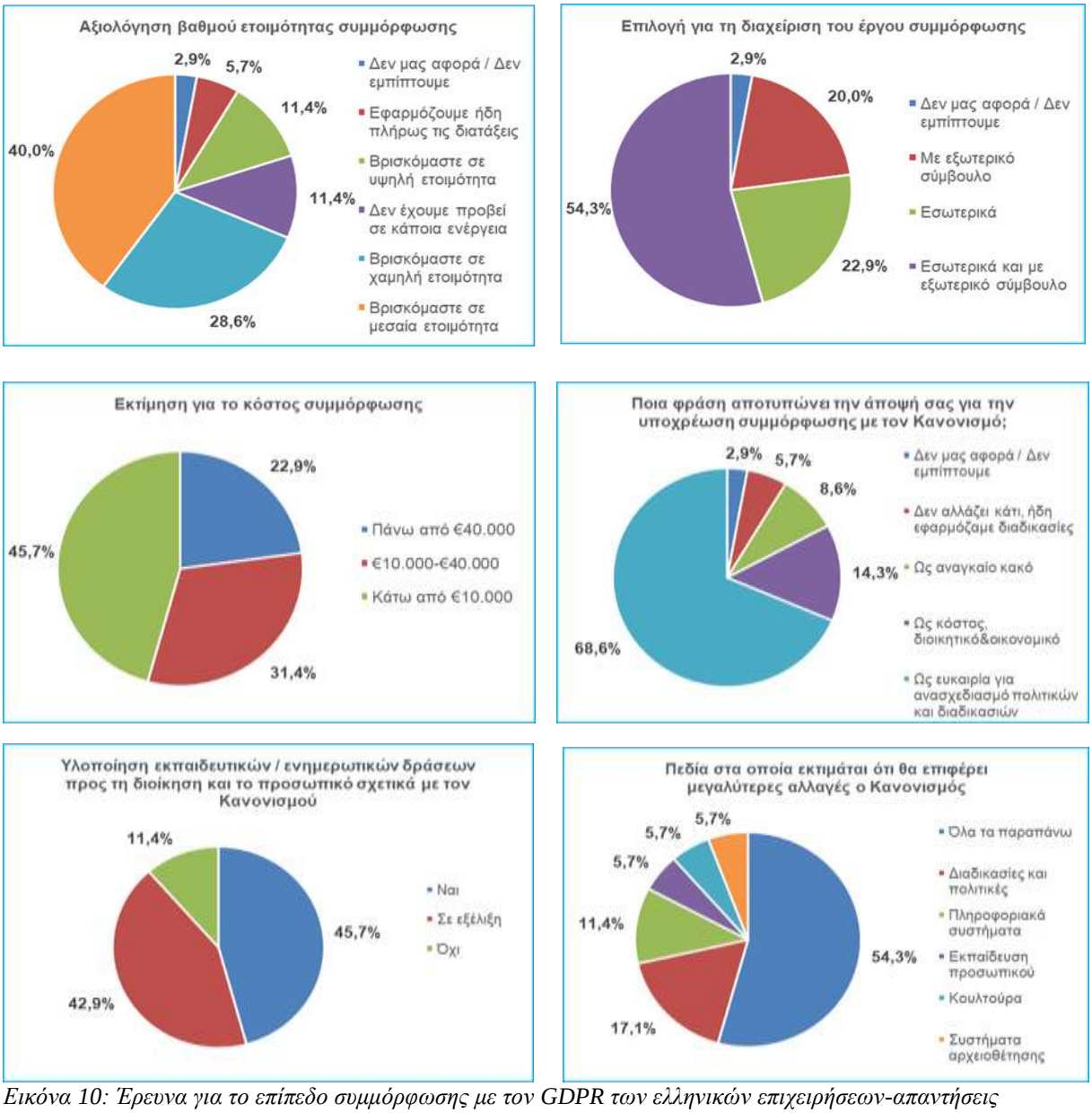
✓ Εκτιμάται ότι ακόμα και μεταξύ των επιχειρήσεων που δηλώνουν ότι γνωρίζουν τον ορισμό, ενδέχεται να περιλαμβάνονται αρκετές που **νομίζουν ότι κατέχουν σχετική γνώση**, ενώ στην πραγματικότητα δεν έχουν.

✓ Σχεδόν **1 στις 3 επιχειρήσεις δηλώνει ότι δεν επεξεργάζεται προσωπικά δεδομένα,** εκτός από εκείνα των εργαζομένων της (π.χ. πελατών και προμηθευτών). Αξιοσημείωτο είναι - και αυτήν την περίπτωση - το υψηλότερο ποσοστό των τουριστικών επιχειρήσεων (40%).

✓ Σχεδόν **1 στις 4 επιχειρήσεις δηλώνει ότι δεν συμμορφώνεται στον Κανονισμό.** Σε συνδυασμό με ποσοστό 58% των επιχειρήσεων που δηλώνει ότι συμμορφώνεται.

5.6.2 Η έρευνα του ΣΕΒ

Η συγκεκριμένη - περιορισμένης έκτασης - έρευνα πραγματοποιήθηκε την περίοδο από 13 έως 23 Φεβρουαρίου 2018, αποκλειστικά σε επιχειρήσεις μέλη του ΣΕΒ και το δείγμα ανέρχεται σε 35 επιχειρήσεις. Παρακάτω παρουσιάζονται τα κυριότερα συμπεράσματα, τόσο για το βαθμό ετοιμότητας των επιχειρήσεων, όσο και για μια σειρά από άλλα ποιοτικού χαρακτήρα στοιχεία:



Εικόνα 10: Έρευνα για το επίπεδο συμμόρφωσης με τον GDPR των ελληνικών επιχειρήσεων-απαντήσεις και σε άλλες ερωτήσεις συναφείς με την συμμόρφωση Πηγή: Έρευνα ΣΕΒ, Φεβ. 2018

Ειδικότερα:

- ✓ **8 στις 10 επιχειρήσεις αξιολογούν ως μέτριο ή χαμηλό το βαθμό ετοιμότητας** ως προς τη συμμόρφωση με τον Κανονισμό, ή - χειρότερα - δεν έχουν προβεί ακόμα σε κάποια ενέργεια.
- ✓ **Περισσότερες από 1 στις 2 επιχειρήσεις δηλώνουν ότι διαχειρίζονται το έργο συμμόρφωσης συνδυαστικά, τόσο με ίδιες δυνάμεις, όσο και με τη χρήση εξωτερικού συμβούλου**. Το γεγονός αυτό μπορεί να ερμηνευθεί ως μια «ανασφάλεια» των επιχειρήσεων ως προς τη δυνατότητά τους να ανταποκριθούν στις διατάξεις του Κανονισμού και για το λόγο αυτό επιλέγουν και τη συμβολή ενός εξειδικευμένου εξωτερικού συμβούλου.
- ✓ Ως προς το **κόστος συμμόρφωσης, αυτό εκτιμάται μικρότερο από €40 χιλ. για το 77,1% του δείγματος**. Σημειώνεται ότι όλες οι επιχειρήσεις που δήλωσαν κόστος μεγαλύτερο από €40 χιλ. παρουσιάζουν Κύκλο Εργασιών πάνω από €100 εκ. (συνεπώς, διαφαίνεται μια συσχέτιση μεταξύ μεγέθους επιχείρησης και κόστους συμμόρφωσης).
- ✓ **2 στις 3 επιχειρήσεις αντιμετωπίζουν τον Κανονισμό ως ευκαιρία για ανασχεδιασμό των πολιτικών και διαδικασιών τους**, μήνυμα το οποίο μπορεί να εκληφθεί ως ιδιαίτερα αισιόδοξο, καθώς αποτυπώνει μια θετική νοοτροπία / προσέγγιση προς τον Κανονισμό, ισχυροποιώντας την πεποίθηση του ΣΕΒ περί αξιοποίησης του Κανονισμού και επίτευξης της επονομαζόμενης «έξυπνης συμμόρφωσης», βασισμένη σε τρεις αρχές που αναδεικνύουν εύληπτα και τα οφέλη που προκύπτουν από τον Κανονισμό (αναπτύσσεται αναλυτικά στην ενότητα 5.3).
- ✓ Οι **επιχειρήσεις αναγνωρίζουν την αναγκαιότητα πραγματοποίησης εκπαιδευτικών δράσεων**, προκειμένου να διαχυθούν στον οργανισμό τους οι νέες υποχρεώσεις και οι σχετικές πολιτικές και διαδικασίες που προκύπτουν από τον Κανονισμό: σχεδόν όλες έχουν ήδη προβεί, ή υλοποιούν, σχετικές δράσεις (88,6%).
- ✓ Η υψηλή τεχνικότητα και ο συνδυασμός ενεργειών που απαιτείται για την επίτευξη συμμόρφωσης στον Κανονισμό αναδεικνύεται εύληπτα στην έρευνα: **1 στις 2 επιχειρήσεις** δηλώνει ότι η **διαδικασία συμμόρφωσης περιλαμβάνει πολλαπλές δράσεις**, σε διαφορετικά αντικείμενα και επίπεδα, όπως σε: διαδικασίες και πολιτικές, πληροφοριακά συστήματα, εκπαίδευση προσωπικού, εταιρική κουλτούρα και συστήματα αρχειοθέτησης.

5.7 Σύνοψη

Εν κατακλείδι, με την κατάλληλη προετοιμασία και κατανόηση της μεθοδολογίας σε θεωρητικό επίπεδο, που συνιστούν έναν «οδικό χάρτη», ο οποίος, εφόσον κατά την εφαρμογή του ληφθούν υπόψη οι ιδιαιτερότητες και οι ειδικές ανάγκες της κάθε οικονομικής οντότητας και στο μέτρο που θα υλοποιηθεί, εξασφαλίζει στην επιχείρηση ομαλή προσαρμογή στις απαιτήσεις του Κανονισμού και επαρκές, επίπεδο προστασίας προσωπικών δεδομένων. Μέσω της εφαρμογής των κατάλληλων τεχνικών και της εκπαίδευσης του ανθρώπινου δυναμικού τους, οι επιχειρήσεις ενισχύουν την ασφάλεια των προσωπικών τους δεδομένων και εξασφαλίζουν τη συνεχή προστασία αυτών.

Από τις δύο έρευνες που παρουσιάστηκαν, παρατηρούμε πως για πολλούς το GDPR αποτελεί ευκαιρία για ανασχεδιασμό των πολιτικών και διαδικασιών των επιχειρήσεων, ενώ απαιτείται εντατικοποίηση των προσπαθειών των επιχειρήσεων για την επίτευξη της συμμόρφωσης με τον Κανονισμό. Το συμπέρασμα αυτό, εξάγεται και από την έρευνα που πραγματοποίησε η πανευρωπαϊκή σουηδική εισπρακτική εταιρεία Intrum, όπου το 69% των επιχειρήσεων στην Ελλάδα δεν είναι ενημερωμένες για τον νέο κανονισμό, ενώ 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.[14] Με βάση τα παραπάνω, το συνολικό κόστος συμμόρφωσης με τον GDPR για τις επιχειρήσεις στην Ευρώπη εκτιμάται σε 198 δισ. ευρώ.

[14] http://www.kathimerini.gr «Ανέτοιμοι για τον κανονισμό προστασίας προσωπικών δεδομένων»

Εικόνα 11:Επιχειρήσεις σε Ελλάδα και Ευρώπη που δηλώνουν άγνοια για τον GDPR

Βέβαια, όλα τα παραπάνω απαιτούν και τα κατάλληλα τεχνολογικά και υποστηρικτικά μέτρα, συστήματα και εφαρμογές, που είναι μεν κοστοβόρα και άρα προσβάσιμα σε μεγάλες κυρίως οικονομικές οντότητες, που όμως θα διευκολύνουν την επιχείρηση στη γρηγορότερη και ασφαλέστερη μετάβαση στον GDPR. Μερικά από αυτά τα συστήματα, περιγράφονται αναλυτικά στο κεφάλαιο που ακολουθεί.

ΚΕΦΑΛΑΙΟ 6 : ΛΟΓΙΣΜΙΚΑ ΥΠΟΣΤΗΡΙΞΗΣ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗΣ ΤΟΥ ΝΕΟΥ ΚΑΝΟΝΣΜΟΥ ΑΠΟ ΜΕΓΑΛΕΣ ΕΤΑΙΡΕΙΕΣ ΛΟΓΙΣΜΙΚΩΝ

6.1 Εισαγωγή

Η ραγδαία ανάπτυξη που γνώρισε τα τελευταία χρόνια ο τομέας των ηλεκτρονικών υπηρεσιών σε συνδυασμό με την ευρεία χρήση του διαδικτύου και των social media, έχει συμβάλει σημαντικά στην εξέλιξη της οικονομίας και της κοινωνίας, ταυτόχρονα όμως έχει δημιουργήσει νέα προβλήματα που χρήζουν αντιμετώπισης, όπως αυτό της παραβίασης των προσωπικών δεδομένων. Οι οικονομικές οντότητες, έχουν ενσωματώσει πλέον στο βασικό τους αντικείμενο όλα

τα νέα τεχνολογικά επιτεύγματα, δημιουργώντας πολλές βάσεις δεδομένων με προσωπικά δεδομένα. Ωστόσο, αυτές οι νέες βάσεις δεδομένων αποτελούν συχνά βορά για κυβερνοεπιθέσεις από επιτήδειους χάκερς. Έτσι για να προστατευτούν οι οργανισμοί έχουν θεσπίσει πολλαπλά επίπεδα ασφαλείας γύρω από τη βάση δεδομένων τους, είτε χρησιμοποιώντας τείχος προστασίας (firewall), είτε συστήματα ανίχνευσης εισβολών και κατάλληλη κατάτμηση δικτύων, επιδιώκοντας έτσι οι εισβολείς να μην καταφέρουν να φτάσουν απευθείας στις βάσεις δεδομένων της επιχείρησης. Ωστόσο, καθώς οι συνήθεις περίμετροι του δικτύου γίνονται πιο πολύπλοκες και ο αριθμός των ατόμων (διαχειριστές, προγραμματιστές και συνεργάτες) που έχουν άμεση πρόσβαση στις βάσεις δεδομένων όλο και αυξάνεται, καθίσταται πολύ σημαντική η άμεση διασφάλιση των βάσεων δεδομένων. Προκειμένου να περιοριστούν οι «ευάλωτες» περιοχές και να μειωθεί ο αριθμός των τρόπων με τους οποίους οι «επιτιθέμενοι εισβολείς» μπορούν να φτάσουν στις βάσεις δεδομένων, είναι εξαιρετικά σημαντικό να επιβάλλεται η ασφάλεια όσο το δυνατόν πιο κοντά στα δεδομένα.

Συνεπώς, οι ιδιωτικές επιχειρήσεις και οι κρατικοί οργανισμοί, πέραν της προετοιμασίας, εκπαίδευσης και των μεθοδολογιών που οφείλουν να ακολουθήσουν ως προς την συμμόρφωση με τον νέο Κανονισμό, οφείλουν και να εξετάσουν τον τρόπο με τον οποίο αναπτύσσονται τα συστήματά τους, τις εφαρμογές τις οποίες χρησιμοποιούν, όπου ενδέχεται να μην έχουν τον πηγαίο κώδικά τους και να εξαρτώνται από τρίτους, είτε εντός είτε εκτός της ΕΕ.

Την ανάγκη αυτή των οικονομικών οντοτήτων θέλουν να εκμεταλλευτούν οι μεγαλύτερες εταιρείες hardware και software λογισμικών είτε αναπτύσσοντας έτοιμα προγράμματα και βάσεις δεδομένων που ενσωματώνουν τις διατάξεις του νέου Κανονισμού, είτε αναβαθμίζοντας τα ήδη υφιστάμενα προγράμματά τους, ώστε να συμπεριλάβουν αυτόματα και τις εταιρείες που τα χρησιμοποιούν ήδη, είτε παρέχοντας έτοιμες λύσεις και μεθοδολογίες, προκειμένου να διευκολύνουν και να υποστηρίξουν τους οργανισμούς στη γρηγορότερη μετάβαση και συμμόρφωση με τον GDPR.

Στις παρακάτω σελίδες θα γίνει προσπάθεια να περιγράφουν οι βασικότερες εφαρμογές που έχουν αναπτύξει κάποιες από τις μεγαλύτερες εταιρείες στην ανάπτυξη λογισμικών, σχετικά με την συμμόρφωση με τον GDPR για την πρόληψη

και έγκαιρη ανίχνευση «επιθέσεων». Ακόμη θα γίνει αναφορά στις συμβουλευτικές μεθόδους και υπηρεσίες που παρέχουν εταιρείες τρίτων για την διευκόλυνση των οικονομικών οντοτήτων, τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα στην ενσωμάτωση του GDPR στο εσωτερικό τους.

6.2 Λογισμικά της εταιρείας ORACLE

Η Oracle υπήρξε και εξακολουθεί να είναι αδιαμφισβήτητος ηγέτης στην ασφάλεια των δεδομένων για δεκαετίες και έχει αναπτύξει καινοτόμα προϊόντα ασφάλειας δεδομένων για να βοηθήσει τις επιχειρήσεις να αντιμετωπίσουν επιθέσεις από διάφορους φορείς απειλών. Ήταν η πρώτη που εισήγαγε ελέγχους, όπως την «ασφάλεια επιπέδου γραμμής» (Row-level security), την κρυπτογράφηση δεδομένων (Transparent data encryption) για τον περιορισμό της προνομιακής πρόσβασης των χρηστών σε ευαίσθητες πληροφορίες, την προνομιακή ανάλυση (Privilege Analysis) και το τείχος προστασίας δεδομένων (Database Firewall).

Οι τεχνολογίες και τα προϊόντα της Oracle μπορούν να βοηθήσουν τους οργανισμούς να επιταχύνουν τη συμμόρφωση με τον GDPR αντιμετωπίζοντας τις προκλήσεις μέσω της αυτόματης, ολοκληρωμένης και αποδοτικής σουίτας τεχνολογίας και προϊόντων. Τα προϊόντα της Oracle καλύπτουν 3 βασικές παραμέτρους για τη συμμόρφωση με τον GDPR: την Αξιολόγηση (Assess), την Πρόληψη (Prevent) και την Ανίχνευση (Detect), που αν συνδυαστούν κατάλληλα, οδηγούν στη Μέγιστη Προστασία των προσωπικών δεδομένων. Ειδικότερα:

1) **Αξιολόγηση (Assess)** κινδύνων ασφαλείας. Σύμφωνα με το άρθρο 35 του νέου Κανονισμού προβλέπετε εκτίμηση των επιπτώσεων για ορισμένους τύπους επεξεργασίας δεδομένων. Μία από τις προκλήσεις είναι να προσδιοριστεί τι πρέπει να αξιολογηθεί, επειδή οι εφαρμογές βάσεων δεδομένων περιέχουν συνήθως πολλά σημεία εισόδου και έχουν προσωπικά δεδομένα κατανεμημένα σε πολλαπλές στήλες και πίνακες με «χαλαρά» καθορισμένο έλεγχο πρόσβασης.

Η τεχνολογία και τα προϊόντα της Oracle Database Security βοηθούν στην αντιμετώπιση αυτής της πρόκλησης παρέχοντας εργαλεία για την αξιολόγηση πολλών πτυχών των δεδομένων της εφαρμογής, όπως:

- ✓ Ανακάλυψη πινάκων και στηλών που περιέχουν «προσωπικά δεδομένα»

✓ Διαμόρφωση των βάσεων δεδομένων για τον προσδιορισμό του συνολικού προφίλ ασφαλείας

✓ Ανάλυση των ρόλων και των δικαιωμάτων των βάσεων δεδομένων για τον καθορισμό του τρόπου με τον οποίο οι ελεγκτές, οι επεξεργαστές, τα τρίτα μέρη, τα δεδομένα και οι παραλήπτες μπορούν να έχουν πρόσβαση σε προσωπικά δεδομένα

Τα εργαλεία που παρέχει η Oracle για την αξιολόγηση είναι:

➢ Oracle Application Data Modeling (Αξιολόγηση ευαίσθητων δεδομένων), όπου αυτοματοποιεί τον εντοπισμό των στηλών που περιέχουν ευαίσθητα δεδομένα προσωπικού χαρακτήρα και τις αντίστοιχες σχέσεις γονέα- παιδιού που ορίζονται στη βάση δεδομένων, χρησιμοποιώντας ενσωματωμένα πρότυπα, όπως αριθμούς πιστωτικών καρτών και εθνικά αναγνωριστικά. Μόλις εντοπιστούν τα προσωπικά δεδομένα, τότε είναι δυνατή η εφαρμογή των σχετικών ελέγχων, είτε προληπτικά είτε αναγνωριστικά. Το αποτέλεσμα είναι ένα πλήρες σύνολο «ευαίσθητων» στηλών μαζί με τις σχέσεις τους, εξασφαλίζοντας ότι η ακεραιότητα της εφαρμογής διατηρείται από τους ελέγχους προστασίας δεδομένων.

➢ Oracle Database Vault Privilege Analysis (Αξιολόγηση της Προνομιακής Πρόσβασης), Μόλις προσδιοριστούν τα προσωπικά δεδομένα, είναι σημαντικό να εντοπιστούν οι χρήστες, συμπεριλαμβανομένων και των διαχειριστών, οι οποίοι μπορούν όχι μόνο να έχουν πρόσβαση αλλά και να επεξεργάζονται τα προσωπικά δεδομένα. Ωστόσο, κατά τη διάρκεια της διαδικασίας σχεδιασμού και συντήρησης της εφαρμογής, ενδέχεται να χορηγηθούν εκ παραδρομής πρόσθετα δικαιώματα στους χρήστες. Έτσι, με τη χρήση της Oracle Database Vault Privilege Analysis επιτυγχάνεται αύξηση της ασφάλειας των εφαρμογών, αφού αναγνωρίζει τα πραγματικά δικαιώματα των χρηστών που χρησιμοποιούνται κατά την εκτέλεση. Τα δικαιώματα που έχουν αναγνωριστεί ως αχρησιμοποίητα μπορούν να αξιολογούνται για πιθανή ανάκληση, συμβάλλοντας στην επίτευξη ενός «μοντέλου ελαχίστων προνομίων».

➢ Oracle Database Lifecycle Management Pack (Αξιολόγηση της ρύθμισης των παραμέτρων της βάσης δεδομένων). Όλες οι βάσεις δεδομένων αποτελούνται από ένα πλήθος παραμέτρων διαμόρφωσης για να ανταποκρίνονται στις ευρείες απαιτήσεις ασφαλείας. Έτσι, οι επιχειρήσεις πρέπει να ελέγξουν όλες τις ρυθμίσεις των βάσεων δεδομένων που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένων των προεπιλεγμένων κωδικών πρόσβασης των λογαριασμών, την κατάσταση και τα

προφίλ του λογαριασμού. Με το συγκεκριμένο εργαλείο, μπορούν να εκτελεστούν περισσότεροι από 100 έλεγχοι πολιτικής στις βάσεις δεδομένων της Oracle, να εντοπιστούν οι τάσεις και να πραγματοποιηθούν εξατομικευμένοι έλεγχοι διαμόρφωσης για να συμπληρώσουν τους ελέγχους που παρέχει η Oracle.

- Oracle Database Security Assessment Tool (Αξιολόγηση του προφίλ ασφάλειας των βάσεων δεδομένων)**.** Σύμφωνα με το άρθρο 36 του GDPR, ανάλογα με την ευαισθησία των δεδομένων, οι επιχειρήσεις ενδέχεται να χρειαστούν την έγκριση μιας Εποπτικής Αρχής πριν από την επεξεργασία ορισμένων προσωπικών πληροφοριών. Η πρόκληση είναι να δημιουργηθεί γρήγορα μια ευδιάκριτη έκθεση αναφοράς σχετικά με την προστασία της ιδιωτικής ζωής και της ασφάλειας για να υποβληθεί στην Εποπτική Αρχή. Με το συγκεκριμένο εργαλείο αναλύεται όχι μόνο η διαμόρφωση αλλά και ο τρόπος εφαρμογής ορισμένων πολιτικών ασφαλείας. Στη συνέχεια, παρουσιάζονται τα ευρήματά του ιεραρχημένα ώστε να μπορούν να υποβληθούν στην Εποπτική Αρχή. Αυτές οι πληροφορίες μπορούν να συμβάλουν σημαντικά στη μελέτη της εκτίμησης των επιπτώσεων στην προστασία των δεδομένων.

2) **Πρόληψη** (Prevent). Η Oracle παρέχει μια εύκολη στη χρήση σειρά προληπτικών ελέγχων που βοηθά τους οργανισμούς να εφαρμόσουν τις βασικές προληπτικές τεχνικές σύμφωνα με το GDPR, συμπεριλαμβανομένης της κρυπτογράφησης, της ψευδωνυμοποίησης, της ανωνυμίας, του προνομιακού ελέγχου των χρηστών, του λεπτομερούς ελέγχου πρόσβασης και της απόκρυψης δεδομένων.

- Transparent Data Encryption (TDE): (Κρυπτογράφηση δεδομένων). Το συγκεκριμένο εργαλείο, αντιμετωπίζει τα όσα ορίζει ο GDPR στο άρθρο 32, σχετικά με την χρήση της κρυπτογράφησης ως μία από τις τεχνικές προστασίας δεδομένων απευθείας στη βάση δεδομένων. Κρυπτογραφεί τα δεδομένα αυτόματα όταν είναι καταγεγραμμένα στο χώρο αποθήκευσης, συμπεριλαμβανομένων των αντιγράφων ασφαλείας, των εξαχθέντων δεδομένων και των αρχείων καταγραφής. Τα κρυπτογραφημένα δεδομένα αντίστοιχα αποκρυπτογραφούνται όταν διαβάζονται από το χώρο αποθήκευσης. Αυτή η δυνατότητα αυτόματης κρυπτογράφησης-αποκρυπτογράφησης σε επίπεδο βάσης δεδομένων καθιστά τη λύση διαφανή σε εφαρμογές βάσης δεδομένων. Τα στοιχεία ελέγχου πρόσβασης που επιβάλλονται στη βάση δεδομένων και τα επίπεδα εφαρμογής παραμένουν σε ισχύ.

- Oracle Key Vault (OKV) (Διαχείριση κεντρικών κλειδιών κρυπτογράφησης). Το Oracle Key Vault (OKV) παρέχει κεντρικό έλεγχο στα δεδομένα που είναι κρυπτογραφημένα με το προηγούμενο εργαλείο (TDE).

- Oracle Database Network Encryption and Data Integrity (Κρυπτογράφηση δεδομένων σε μεταφορά). Για να πληρούνται οι απαιτήσεις του άρθρου 32 του GDPR για την προστασία των προσωπικών δεδομένων στη μετάδοση, η συγκεκριμένη εφαρμογή βοηθά τις επιχειρήσεις και τους υπευθύνους να κρυπτογραφούν δεδομένα και να αποτρέπουν την απώλεια δεδομένων, την επανάληψη και τις ενδιάμεσες επιθέσεις.

- Data Redaction (Ψευδωνυμοποίηση δεδομένων). Για παράδειγμα, ένα χαρακτηριστικό γνώρισμα σε μια στήλη πίνακα που αντιπροσωπεύει ένα υποκείμενο δεδομένων μπορεί να τροποποιηθεί ή ένας πίνακας που περιέχει πολλαπλά χαρακτηριστικά που μπορούν να βοηθήσουν στη δημιουργία του συνδέσμου με το αρχικό υποκείμενο δεδομένων μπορεί να προστατευθεί με τέτοιο τρόπο ώστε να μην είναι δυνατή η σύνδεση του συνόλου δεδομένων με το υποκείμενο των δεδομένων. (GDPR άρθρο 32). Η χρήση του Data Redaction μπορεί να βοηθήσει στην αντιμετώπιση της υποκλοπής ερωτημάτων εφαρμογής στη βάση δεδομένων, παρέχοντας επιλεκτική και άμεση επεξεργασία των προσωπικών δεδομένων στα αποτελέσματα των ερωτημάτων SQL πριν επιστρέψει στις εφαρμογές, ώστε οι μη εξουσιοδοτημένοι χρήστες να μην μπορούν να δουν τα δεδομένα. Το συγκεκριμένο πρόγραμμα δεν επηρεάζει τις λειτουργικές δραστηριότητες της βάσης δεδομένων, όπως η δημιουργία αντιγράφων ασφαλείας και η επαναφορά, η αναβάθμιση και η ενημερωμένη έκδοση κώδικα, καθώς δεν μεταβάλλονται τα σταθερά δεδομένα. Οι πολιτικές της Oracle Data Redaction επιβάλλονται απευθείας στον πυρήνα της βάσης δεδομένων, οδηγώντας σε αυστηρότερη ασφάλεια και καλύτερη απόδοση. Επιτρέπει επίσης στο διαχειριστή να καθορίσει τις συνθήκες υπό τις οποίες τα πραγματικά δεδομένα πρέπει να επιστραφούν στους εξουσιοδοτημένους αποδέκτες.

- Oracle Data Masking and Subsetting (Ανωνυμοποίηση και ελαχιστοποίηση). Το συγκεκριμένο εργαλείο μπορεί να χρησιμοποιηθεί για την αποδέσμευση των προσωπικών δεδομένων του Υπευθύνου Προστασίας Δεδομένων και για τον περιορισμό της έκθεσης προσωπικών δεδομένων σε λιγότερο προστατευμένα περιβάλλοντα. Μία από τις προκλήσεις της ανωνυμοποίησης είναι ότι αν δεν γίνει σωστά, θα μπορούσε να σπάσει την ακεραιότητα των δεδομένων των εφαρμογών και των βάσεων δεδομένων. Το Oracle Data Masking and Subsetting

αντιμετωπίζει τον κίνδυνο τα μη- ταυτοποιημένα ή κωδικοποιημένα δεδομένα να μην είναι χρησιμοποιήσιμα για τους επεξεργαστές και τους προγραμματιστές. παρέχοντας μια ολοκληρωμένη και επεκτάσιμη βιβλιοθήκη με μορφές ανωνυμοποίησης και κάλυψης, μετασχηματισμούς και πρότυπα εφαρμογών. Τα προσωπικά δεδομένα και άλλες σημαντικές πληροφορίες, όπως αριθμοί πιστωτικών καρτών, εθνικά αναγνωριστικά στοιχεία και άλλες πληροφορίες προσωπικής ταυτοποίησης, μπορούν εύκολα να καλυφθούν με μια άλλης μορφής βιβλιοθήκη κάλυψης και ανωνυμοποίησης.

- Oracle Database Vault: (Έλεγχος των Προνομιακών Χρηστών και επιβολή του Διαχωρισμού των Υποχρεώσεων), όπου ενσωματώνει τον έλεγχο πρόσβασης των χρηστών εντός της βάσης δεδομένων της Oracle, δημιουργώντας πυρήνες που περιορίζουν την πρόσβαση στα δεδομένα μόνο σε εξουσιοδοτημένο προσωπικό και υπό ορισμένες συνθήκες. Ταυτόχρονα επιτρέπει στις βάσεις δεδομένων να εκτελούν τις κανονικές λειτουργικές τους δραστηριότητες, όπως την επιδιόρθωση, την εισαγωγή, την εξαγωγή και την δημιουργία αντιγράφων ασφαλείας χωρίς πρόσβαση στα προσωπικά δεδομένα.
- Oracle Virtual Private Database (Επιλεκτική απόκρυψη δεδομένων). Η συγκεκριμένη εφαρμογή παρέχει προσωρινές προληπτικές τεχνικές, όπως φιλτράρισμα και απόκρυψη ενός υποσυνόλου δεδομένων για την αντιμετώπιση περιπτώσεων υποκλοπής δεδομένων ή εμφάνισής τους σε μη εξουσιοδοτημένους χρήστες. Έτσι περιορίζεται το μέγεθος της ζημιάς, σε περίπτωση που υπάρχει ένα σφάλμα προγραμματισμού που επιτρέπει στους χρήστες να μην βλέπουν μόνο τα δικά τους δεδομένα, αλλά και τα δεδομένα άλλων χρηστών.
- Oracle Label Security (Έλεγχος Πρόσβασης) όπου βοηθά τους οργανισμούς να ταξινομούν τα στοιχεία Προσωπικών Δεδομένων αναθέτοντας ετικέτες με βάση την εμπιστευτικότητα (όπως οι δημόσιες, ευαίσθητες ή εξαιρετικά εμπιστευτικές πληροφορίες) ή περιοχές (όπως Βόρεια Αμερική, Ευρώπη ή Ασία-Ειρηνικός).
- Oracle Real Application Security (RAS) (Διευκόλυνση της ολοκλήρωσης του ελέγχου πρόσβασης). Ο υπεύθυνος επεξεργασίας πρέπει να επαληθεύσει την ταυτότητα του αιτούντος υποκειμένου δεδομένων στο πλαίσιο των ηλεκτρονικών υπηρεσιών, προτού δώσει πρόσβαση στα προσωπικά δεδομένα[15]. Στις σύγχρονες

[15] Αιτιολογική σκέψη 64 του GDPR

εφαρμογές τριών επιπέδων, η επαλήθευση του διαδικτυακού πλαισίου της ταυτότητας ενός χρήστη αποτελεί πρόκληση, επειδή συνήθως οι εφαρμογές και οι διακομιστές εφαρμογών συνδέονται στη βάση δεδομένων ως ένας χρήστης μιας βάσης δεδομένων που καθιστά δύσκολο τον εντοπισμό του δημιουργού χρήστη. Το Oracle Real Application Security (RAS) αντιμετωπίζει αυτή την ανησυχία παρέχοντας ένα μοντέλο εξουσιοδότησης βάσει πολιτικής που αναγνωρίζει τους χρήστες, τα δικαιώματα και τους ρόλους σε επίπεδο εφαρμογής μέσα στη βάση δεδομένων. Με την ενσωματωμένη υποστήριξη για την ασφαλή διάδοση των πληροφοριών των χρηστών στη βάση δεδομένων, το RAS επιτρέπει στις πολιτικές ασφαλείας των δεδομένων να εκφράζονται απευθείας από την άποψη των χρηστών της εφαρμογής, των ρόλων τους και των πλαισίων ασφαλείας.

3) **Παρακολούθηση εντοπισμού παραβιάσεων** (DETECT) Τα άρθρα 30 και 33 του GDPR ορίζουν ότι οι οργανισμοί πρέπει να τηρούν αρχείο των δραστηριοτήτων επεξεργασίας τους. Αυτό μπορεί να επιτευχθεί μόνο με τη συνεχή παρακολούθηση και τον έλεγχο δραστηριοτήτων σχετικά με τα προσωπικά δεδομένα. Αυτά τα δεδομένα μπορούν στη συνέχεια να χρησιμοποιηθούν για την έγκαιρη ενημέρωση των αρχών σε περίπτωση παραβίασης. Εκτός από τον υποχρεωτικό έλεγχο και τις έγκαιρες ειδοποιήσεις, ο GDPR απαιτεί επίσης οι οργανισμοί να τηρούν αρχεία ελέγχου υπό τον έλεγχό που πραγματοποίησαν. Ένας κεντρικός έλεγχος των αρχείων ελέγχου αποτρέπει τους εισβολείς ή τους κακόβουλους χρήστες να καλύψουν τα ίχνη της ύποπτης δραστηριότητάς τους διαγράφοντας τα αρχεία τοπικού ελέγχου.

Η Oracle Database Security παρέχει έναν εκτεταμένο μηχανισμό συλλογής και υποβολής εκθέσεων για την κάλυψη των απαιτήσεων παρακολούθησης του GDPR. Το Oracle Audit Vault and Database Firewall (AVDF) είναι μια πλατφόρμα ελέγχου και προστασίας νέας γενιάς που παρέχει ολοκληρωμένη και ευέλικτη παρακολούθηση μέσω της ενοποίησης δεδομένων ελέγχου από βάσεις δεδομένων Oracle και μη Oracle, λειτουργικά συστήματα, συστήματα αρχείων και εφαρμογή συγκεκριμένων δεδομένων ελέγχου. Ταυτόχρονα, το Oracle Database Firewall μπορεί να λειτουργήσει ως η πρώτη γραμμή υπεράσπισης στο δίκτυο, επιβάλλοντας την αναμενόμενη συμπεριφορά των εφαρμογών, βοηθώντας στην πρόληψη της εισόδου SQL, της παράκαμψης εφαρμογής και άλλων κακόβουλων δραστηριοτήτων από την πρόσβαση στη βάση δεδομένων.

Επιπλέον, μπορεί να ενοποιήσει τα δεδομένα ελέγχου από πολλαπλές βάσεις δεδομένων και να παρακολουθήσει την κυκλοφορία των εντολών που δεν είναι εξουσιοδοτημένες. Οι υπεύθυνοι προστασίας δεδομένων και οι υπεύθυνοι επεξεργασίας μπορούν να καθορίσουν τις συνθήκες υπό τις οποίες μπορούν να εγγραφούν οι ειδοποιήσεις σε πραγματικό χρόνο, προσπαθώντας να προσελκύσουν τους εισβολείς με τις μη φυσιολογικές δραστηριότητες.

4) **Μέγιστη προστασία με διαφάνεια, ακρίβεια, απόδοση και κλίμακα** (Maximum Protection).

Δεδομένου ότι οι σύγχρονες εφαρμογές περιέχουν πολλά στοιχεία, όπως πύλες ιστού, διακομιστές μεσολάβησης, διακομιστές εφαρμογών και διακομιστές βάσεων δεδομένων, ο καθορισμός και η εφαρμογή όλων των ελέγχων ασφαλείας σε περιβάλλον πολλαπλών στρωμάτων είναι ένα δύσκολο έργο. Η συγκέντρωση όλων αυτών των διαφορετικών ελέγχων ασφάλειας και τεχνολογιών από διάφορους προμηθευτές αποτελεί πρόκληση ενοποίησης και διαχείρισης για τους οργανισμούς. Η Oracle Database Security αντιμετωπίζει αυτή την πρόκληση ορίζοντας τα στοιχεία ελέγχου πιο κοντά στα δεδομένα και επιβάλλοντας την ασφάλεια στις βάσεις δεδομένων. Οι περισσότεροι έλεγχοι προστασίας δεδομένων που προσφέρει η Oracle ενσωματώνονται στη βάση δεδομένων της Oracle, απλοποιώντας έτσι το σχεδιασμό και την ανάπτυξη, βελτιώνοντας την ακρίβεια της προστασίας και ελαχιστοποιώντας την κλίμακα της επίθεσης.

Το Oracle Key Vault και το Oracle Audit Vault and Database Firewall συμπληρώνουν την προστασία δεδομένων στην βάση δεδομένων, συγκεντρώνοντας τον έλεγχο και τη διαχείριση. Είτε πρόκειται για χιλιάδες κλειδιά κρυπτογράφησης και εκατομμύρια αρχεία ελέγχου, είτε για διαφορετικούς τύπους πολιτικών ασφαλείας, αυτά τα στοιχεία μπορούν να διαχειρίζονται κεντρικά, απλοποιώντας σε μεγάλο βαθμό τις εργασίες που σχετίζονται με τη διοίκηση. Επίσης μέσω του Oracle Enterprise Manager (EM) παρέχεται ένα ενιαίο γραφικό περιβάλλον για τη διαχείριση των στοιχείων της Oracle Database Security.Το σημαντικότερο είναι ότι όλα τα στοιχεία ελέγχου της Oracle Database Security είναι καλά ενσωματωμένα για την προστασία των Προσωπικών Δεδομένων. (Oracle Απαραίτητη η ξεκάθαρη στρατηγική it ασφαλείας για τη συμμόρφωση με τον GDPR , Ετήσια Έκδοση 2017)

Στην Ελλάδα, πρόσφατο παράδειγμα αξιοποίησης των εργαλείων της Oracle είναι η συνεργασία της με την εταιρεία παροχής τηλεπικοινωνιών **Wind Ελλάς**, η οποία ολοκλήρωσε επιτυχώς ένα έργο στρατηγικής σημασίας σχετικά με το νέο Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR) της ΕΕ. Το έργο περιλάμβανε, στην πρώτη του φάση, υλοποίηση τεχνολογίας κρυπτογράφησης της Oracle Database στα πιο κρίσιμης σημασίας IT συστήματα της Wind, (σύμφωνα με το άρθρο 32 του νέου Κανονισμού), και στη συνέχεια υλοποίηση τεχνολογίας Oracle Cloud Access Security Broker Service (CASB) για την παρακολούθηση κινδύνου και τη διακυβέρνηση κρίσιμης σημασίας SaaS εφαρμογών, καθώς και την ανακάλυψη Shadow IT εφαρμογών. Το έργο αυτό ήταν μέρος της συνολικής υπάρχουσας στρατηγικής της WIND για τη συμμόρφωσή της με το πλαίσιο GDPR της ΕΕ και πραγματοποιήθηκε με τη συνεργασία του τμήματος Συμβουλευτικών Υπηρεσιών της Oracle.Τα εργαλεία που επέλεξε η Wind είναι το Oracle CASB Service και το Oracle Advanced Security για την ελαχιστοποίηση της έκθεσης σε κίνδυνο και τη διασφάλιση του ελέγχου, που θα της επιτρέψουν να εντοπίσει τυχόν απειλές, ενισχύοντας τα χαρακτηριστικά ασφαλείας του περιβάλλοντος cloud αναφορικά και με το νέο Κανονισμό, με την ελάχιστη δυνατή επίδραση στην απόδοση των IT συστημάτων της[16].

6.3 Λογισμικά της εταιρείας Microsoft

Η εταιρεία Microsoft, γνωστή σε όλους μας για τα πακέτα λογισμικών που παρέχει, αποφάσισε να μην δημιουργήσει μια νέα εφαρμογή που θα αφορά αποκλειστικά τον νέο Κανονισμό. Αντιθέτως επέλεξε την στρατηγική της αξιοποίησης και εμπλούστευσης των ήδη υπαρχόντων συστημάτων και προγραμμάτων της, ενσωματώνοντας εκεί κανόνες συμμόρφωσης με τον GDPR. Η εταιρεία μετά από λεπτομερή μελέτη που διενήργησε πάνω στον νέο Κανονισμό και στις επιπτώσεις του, κατέληξε στα εξής τέσσερα βήματα συμμόρφωσης που πρέπει να ακολουθήσουν οι πελάτες της:

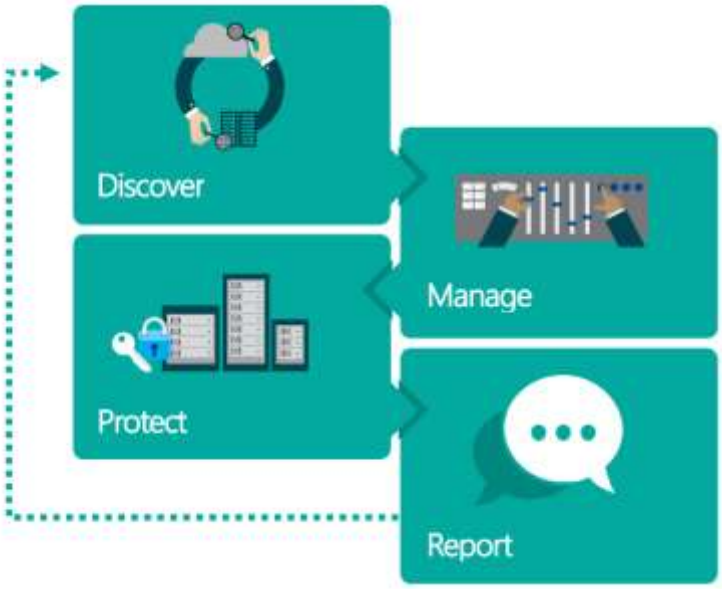
1) **Ανακάλυψη (Discover)**: Προσδιορισμός τους είδους των προσωπικών δεδομένων που κατέχει η εταιρεία και αξιολόγηση εάν το GDPR ισχύει για αυτήν και σε ποιο βαθμό.

[16] Πηγή: www.businessnews.gr/article/91283/wind-oloklirose-ergo-eu-gdpr-me-tehnologies-oracle

2) **<u>Διαχείριση (Manage)</u>**: Καθορισμός του τρόπου χρήσης και πρόσβασης των προσωπικών δεδομένων.

3) **<u>Προστασία (Protect):</u>** Δημιουργία στοιχείων ελέγχου ασφάλειας για την πρόληψη, ανίχνευση και αντιμετώπιση των αδύναμων σημείων και των παραβιάσεων δεδομένων.

4) **<u>Υποβολή έκθεσης (Report)</u>**: Εκτέλεση σε αιτήματα δεδομένων, παραβίαση της αναφοράς και διατήρηση της απαιτούμενης τεκμηρίωσης.



Εικόνα 12: Βήματα συμμόρφωσης με τον GDPR που προτείνει η MICROSOFT

Η εταιρεία δίνει μεγάλη σημασία στο πρώτο βήμα της ανακάλυψης, δηλαδή της σωστής εξακρίβωσης αν η οικονομική οντότητα διαχειρίζεται προσωπικά δεδομένα που άπτονται στον νέο Κανονισμό, καθώς και να εντοπίσει συστήματα στα οποία συλλέγονται αυτά τα δεδομένα και αποθηκεύονται καθώς και τον λόγο για τον οποίο συλλέχτηκαν. Αυτό είναι εφικτό να πραγματοποιηθεί με προϊόντα και υπηρεσίες που προσφέρει η Microsoft, όπως τα Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 και Windows 10. Οι συγκεκριμένες εφαρμογές αποτελούν σήμερα λύσεις που βοηθούν τους οργανισμούς να ανιχνεύσουν και να αξιολογήσουν τις απειλές και τις παραβιάσεις της ασφάλειας και να εκπληρώσουν τις υποχρεώσεις γνωστοποίησης παραβίασης του GDPR, όπως υποστηρίζουν οι ιθύνοντες της εταιρείας. Αναλυτικότερα:

❖ Azure Το Microsoft Azure είναι μια πλήρως διαχειριζόμενη υπηρεσία cloud που λειτουργεί ως σύστημα εγγραφής και ανίχνευσης για τις πηγές δεδομένων του οργανισμού. Μόλις μια πηγή δεδομένων καταχωρηθεί με το Azure Data Catalog, τα δεδομένα της είναι κατηγοριοποιημένα από την υπηρεσία, έτσι ώστε να μπορούν εύκολα να αναζητηθούν. Με το Azure Active Directory διαχειρίζεται η ταυτότητα των δεδομένων και ελέγχεται η πρόσβαση στο Azure, και σε άλλα clouds, δεδομένα και εφαρμογές. Επίσης, μπορούν να εκχωρηθούν προσωρινά δικαιώματα διαχείρισης Just-In-Time (JIT) σε κατάλληλους χρήστες για τη διαχείριση πόρων στο Azure.

Με το Azure Role-Based Access Control (RBAC) δίνεται η δυνατότητα χορήγησης πρόσβασης στα δεδομένα βάσει του ρόλου που έχει αναθέσει ο χρήστης, καθιστώντας ευκολότερη τη χορήγηση μόνο των απαιτούμενων δικαιωμάτων που χρειάζονται οι χρήστες για να εκτελέσουν τις εργασίες τους. Το RBAC μπορεί να προσαρμοστεί ανάλογα με το επιχειρηματικό μοντέλο της επιχείρησης και την ανοχή κινδύνου.

Επιπλέον, με το Azure Security Center παρακολουθούνται συνεχώς οι πόροι της επιχείρησης και παρέχονται χρήσιμες συστάσεις ασφαλείας μέσω της διαδικασίας υλοποίησης των απαιτούμενων στοιχείων ελέγχου, όπως για παράδειγμα, επιτρέποντας την κρυπτογράφηση antimalware ή δίσκου για τους πόρους.

Η πολύ σημαντική έννοια της κρυπτογράφησης δεδομένων στο Azure εξασφαλίζει τα δεδομένα σε κατάσταση αδράνειας και κατά τη μεταφορά. Μπορεί να χρησιμοποιηθεί το Azure Disk Encryption για την κρυπτογράφηση των λειτουργικών συστημάτων και των δίσκων δεδομένων που χρησιμοποιούνται από τα λειτουργικά συστήματα Windows και Linux. Τα δεδομένα προστατεύονται κατά τη μεταφορά μεταξύ μιας εφαρμογής και του Azure, ώστε να παραμένουν πάντα ασφαλή.

Το Azure Key Vault επιτρέπει την προστασία των κρυπτογραφικών κλειδιών, χρησιμοποιώντας μονάδες ασφαλείας υλικού και έχει σχεδιαστεί έτσι ώστε να διατηρείται ο έλεγχος των κλειδιών και συνεπώς και των δεδομένων της επιχείρησης, συμπεριλαμβανομένης της διασφάλισης ότι η Microsoft δεν μπορεί να δει ή να εξαγάγει τα κλειδιά.

Οι ολοκληρωμένες υπηρεσίες με το Azure επιτρέπουν την ταχύτερη και ευκολότερη κατανόηση της γενικής στάσης ασφαλείας, καθώς και την ανίχνευση και διερεύνηση απειλών στο περιβάλλον του cloud. Το Azure Security Center χρησιμοποιεί προηγμένα συστήματα ανάλυσης ασφαλείας, όπως το Azure Log Analytics που παρέχει ρυθμιζόμενες επιλογές ελέγχου και καταγραφής ασφάλειας,

βοηθώντας στη συλλογή και ανάλυση δεδομένων που παράγονται από πόρους σε περιβάλλοντα cloud ή σε χώρους εγκατάστασης. Επίσης, παρέχει πληροφορίες σε πραγματικό χρόνο, χρησιμοποιώντας ολοκληρωμένες έρευνες και προσαρμοσμένους πίνακες ελέγχου, για την εύκολη ανάλυση εκατομμυρίων αρχείων σε όλα τα φορτία και τους διακομιστές, ανεξάρτητα από τη φυσική τους θέση και βοηθά στη διευκόλυνση της γρήγορης ανταπόκρισης και της ενδελεχούς διερεύνησης για τυχόν συμβάντα ασφαλείας.

- **Dynamics 365** Το Dynamics 365 παρέχει αρκετές δυνατότητες προβολής και ελέγχου που μπορούν να χρησιμοποιηθούν μέσω των εργαλείων αναφοράς του Reporting & Analytics του Dynamics 365 για τον εντοπισμό προσωπικών δεδομένων. Περιλαμβάνει έναν Οδηγό αναφοράς για την εύκολη δημιουργία αναφορών χωρίς τη χρήση ερωτημάτων που βασίζονται σε XML ή SQL, ενώ με το Microsoft Power BI, μια αυτοματοποιημένη πλατφόρμα επιχειρηματικής ευφυΐας (BI), οι επιχειρήσεις μπορούν να ανιχνεύσουν, να αναλύσουν και να απεικονίσουν δεδομένα και να τα μοιραστούν με τρίτους.

Επιπλέον, δίνεται η δυνατότητα προστασίας της ακεραιότητας και του απορρήτου των δεδομένων αλλά και η εφαρμογή ασφαλείας βάσει ρόλων, βάσει εγγραφών, για τον καθορισμό της συνολικής πρόσβασης στις πληροφορίες που έχουν οι χρήστες στον οργανισμό.

- **Enterprise Mobility + Security (EMS) Suite** Το Enterprise Mobility + Security διαθέτει τεχνολογίες ασφαλείας που βοηθούν τις επιχειρήσεις να ανακαλύψουν, να ελέγξουν και να διαφυλάξουν τα προσωπικά δεδομένα που κατέχουν, να εντοπίσουν τυχόν «τυφλά» σημεία και να προσδιορίσουν πότε συμβαίνουν παραβιάσεις δεδομένων.

Στην πλειονότητα των παραβιάσεων δεδομένων, οι επιτιθέμενοι αποκτούν πρόσβαση στο εταιρικό δίκτυο μέσω αδύναμων, προεπιλεγμένων ή κλεμμένων διαπιστευτηρίων χρηστών. Με το συγκεκριμένο εργαλείο, η ασφάλεια αρχίζει με την προστασία της ταυτότητας κατά την είσοδο του χρήστη, παρέχοντάς του πρόσβαση υπό όρους ανάλογα με τον κίνδυνο. Το EMS Suite προβάλλει τις δραστηριότητες των χρηστών, των συσκευών και των δεδομένων στις βάσεις δεδομένων και στο cloud και βοηθά στην προστασία των δεδομένων με επιβολή ισχυρών ελέγχων. Για την ολοκληρωμένη πληροφόρηση σχετικά με επιθέσεις και απειλές χρησιμοποιεί αναλύσεις συμπεριφοράς και τεχνολογίες ανίχνευσης αιχμής για τον εντοπισμό και την ανακάλυψη ύποπτων δραστηριοτήτων.

❖ **Office 365** Η πασίγνωστη σε όλους μας πλατφόρμα Office 365 ενσωματώνει ασφάλεια σε όλα τα επίπεδα, από την ανάπτυξη εφαρμογών έως τα φυσικά κέντρα δεδομένων και την πρόσβαση των τελικών χρηστών. Οι εφαρμογές του Office 365 περιλαμβάνουν και ενσωματωμένα χαρακτηριστικά ασφαλείας που απλοποιούν τη διαδικασία προστασίας δεδομένων και την ευελιξία στις επιχειρήσεις να ρυθμίσουν, να διαχειριστούν και να ενσωματώσουν την ασφάλεια με τρόπους που έχουν νόημα για τις επιχειρηματικές τους ανάγκες.

Για παράδειγμα, με τη χρήση του Data Loss Prevention (DLP) στο Office και στο Office 365 μπορούν να εντοπιστούν πάνω από 80 κοινοί ευαίσθητοι τύποι δεδομένων, συμπεριλαμβανομένων των οικονομικών, ιατρικών και προσωπικά αναγνωρίσιμων πληροφοριών. Επιπλέον, το DLP επιτρέπει στους οργανισμούς να ρυθμίζουν τις ενέργειες που πρέπει να αναληφθούν κατά την ταυτοποίηση για να προστατεύσουν τις ευαίσθητες πληροφορίες και να αποτρέψουν την τυχαία αποκάλυψή τους.

Πολλοί έλεγχοι ασφαλείας είναι διαθέσιμοι από προεπιλογή. Το SharePoint και το OneDrive for Business, για παράδειγμα, χρησιμοποιούν κρυπτογράφηση για δεδομένα σε μεταφορά και σε κατάσταση αδράνειας. Με τη βοήθειά τους, οι επιχειρήσεις μπορούν να διαμορφώσουν και να αναπτύξουν ψηφιακά πιστοποιητικά για την απόκρυψη προσωπικών δεδομένων ώστε να περιορίσουν την πρόσβαση σε προσωπικά δεδομένα. Επιπλέον, τα αρχεία καταγραφής ελέγχου του Office 365 επιτρέπουν την παρακολούθηση και τον έλεγχο των δραστηριοτήτων του χρήστη και του διαχειριστή σε όλα τα επίπεδα εργασίας στο Office 365 και βοηθούν στην έγκαιρη ανίχνευση και διερεύνηση ζητημάτων ασφάλειας και συμμόρφωσης.

❖ **SQL Server & Azure SQL Database** Οι βάσεις δεδομένων SQL Server και Azure SQL παρέχουν ελέγχους για τη διαχείριση της πρόσβασης και της εξουσιοδότησης βάσεων δεδομένων σε διάφορα επίπεδα. Συγκεκριμένα, το τείχος προστασίας του Azure SQL Database περιορίζει την πρόσβαση σε μεμονωμένες βάσεις δεδομένων στο διακομιστή βάσης δεδομένων Azure SQL, περιορίζοντας την πρόσβαση αποκλειστικά σε εξουσιοδοτημένες συνδέσεις. Ο έλεγχος ταυτότητας του SQL Server βοηθά στη διασφάλιση ότι μόνο οι εξουσιοδοτημένοι χρήστες με έγκυρα διαπιστευτήρια έχουν πρόσβαση στον διακομιστή της βάσης δεδομένων.

Το Dynamic data masking (DDM) είναι μια ενσωματωμένη δυνατότητα που μπορεί να χρησιμοποιηθεί για τον περιορισμό της ευαίσθητης έκθεσης δεδομένων, αποκρύπτοντας τα δεδομένα όταν έχουν πρόσβαση μη προνομιακοί χρήστες ή

εφαρμογές. Τα καθορισμένα πεδία δεδομένων καλύπτονται από τα αποτελέσματα των ερωτημάτων, ενώ τα δεδομένα στη βάση δεδομένων παραμένουν αμετάβλητα. Για τους χρήστες του Azure SQL Database, μπορεί να ανακαλύψει αυτόματα δυνητικά ευαίσθητα δεδομένα και να προτείνει την εφαρμογή των κατάλληλων «μασκών».

❖ Το Row-level security (RLS) είναι επίσης μια πρόσθετη ενσωματωμένη δυνατότητα που επιτρέπει στους πελάτες SQL Server και SQL Database να εφαρμόσουν περιορισμούς στην πρόσβαση των δεδομένων. Το RLS μπορεί να χρησιμοποιηθεί για να επιτρέψει την εύκολη πρόσβαση σε γραμμές σε έναν πίνακα βάσης δεδομένων, για μεγαλύτερο έλεγχο των χρηστών που έχουν πρόσβαση στα δεδομένα. Δεδομένου ότι η λογική περιορισμού πρόσβασης βρίσκεται στη βαθμίδα βάσης δεδομένων, αυτή η δυνατότητα απλοποιεί σε μεγάλο βαθμό το σχεδιασμό και την εφαρμογή της ασφάλειας εφαρμογών.

❖ Το Always Encrypted είναι μια πρώτη βιομηχανική λειτουργία που έχει σχεδιαστεί για την προστασία ιδιαίτερα ευαίσθητων δεδομένων σε SQL Server και SQL Database. Το Always Encrypted επιτρέπει στους πελάτες να κρυπτογραφούν ευαίσθητα δεδομένα εντός των εφαρμογών του πελάτη και να μην αποκαλύπτουν ποτέ τα κλειδιά κρυπτογράφησης στη μηχανή βάσης δεδομένων. Η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων γίνεται με διαφάνεια σε ένα πρόγραμμα οδήγησης πελάτη που είναι πάντα κρυπτογραφημένο.

❖ Το SQL Database Threat Detection εντοπίζει ανώμαλες δραστηριότητες βάσεων δεδομένων που υποδηλώνουν πιθανές απειλές ασφαλείας στη βάση δεδομένων. Η ανίχνευση απειλών χρησιμοποιεί ένα προηγμένο σύνολο αλγορίθμων για τη συνεχή εκμάθηση και καταγραφή της συμπεριφοράς της εφαρμογής και ενημερώνει αμέσως μόλις εντοπιστεί μια ασυνήθιστη ή ύποπτη δραστηριότητα. Η ανίχνευση απειλών μπορεί να βοηθήσει την επιχείρηση να ανταποκριθεί στην απαίτηση για γνωστοποίηση της παραβίασης δεδομένων σύμφωνα με τον GDPR.

❖ **Windows & Windows Server** Τα Windows 10 και Windows Server 2016 περιλαμβάνουν πρωτοποριακές τεχνολογίες κρυπτογράφησης και λύσεις ταυτότητας και πρόσβασης που επιτρέπουν τη μετακίνηση από κωδικούς πρόσβασης σε πιο ασφαλείς μορφές ελέγχου ταυτότητας:

- Το Windows Defender Antivirus εντοπίζει γρήγορα και προστατεύει από το αναδυόμενο κακόβουλο λογισμικό και μπορεί να βοηθήσει άμεσα στην προστασία των συσκευών όταν παρατηρηθεί μια απειλή σε οποιοδήποτε μέρος του περιβάλλοντος της επιχείρησης.

- Το Windows Defender Advanced Threat Protection, επιτρέπει στις ομάδες λειτουργιών ασφαλείας να εντοπίζουν, να ερευνούν και να ανταποκρίνονται σε παραβιάσεις δεδομένων στο δίκτυο της επιχείρησης. Με το Windows Defender ATP, η επιχείρηση αποκτά προηγμένες δυνατότητες ανίχνευσης, διερεύνησης και απόκρισης με ιστορικά δεδομένα έως και 6 μηνών, ακόμη και όταν τα τελικά σημεία είναι εκτός σύνδεσης, έξω από τον τομέα δικτύου, έχουν επαναληφθεί ή δεν υπάρχουν πια. Το Windows Defender ATP βοηθά τους οργανισμούς να εκπληρώσουν μια βασική απαίτηση του GDPR, το οποίο διαθέτει σαφείς διαδικασίες ανίχνευσης, διερεύνησης και αναφοράς παραβιάσεων δεδομένων.

- Το αρχείο καταγραφής συμβάντων (Windows Event Log) παρέχει πλούσιες δυνατότητες καταγραφής συμβάντων που επιτρέπουν στους διαχειριστές να προβάλλουν καταγεγραμμένες πληροφορίες σχετικά με τις λειτουργίες του λειτουργικού συστήματος, τις εφαρμογές και τις λειτουργίες των χρηστών. Αυτό το σύστημα καταγραφής μπορεί να ρυθμιστεί ώστε να ελέγχει λεπτομερείς ενέργειες χρηστών και εφαρμογών, συμπεριλαμβανομένης της πρόσβασης σε αρχεία, χρήση εφαρμογών και αλλαγές πολιτικών. Το αρχείο καταγραφής συμβάντων των Windows επιτρέπει επίσης στους διαχειριστές να προωθούν γεγονότα από πελάτες και διακομιστές σε κεντρική τοποθεσία για σκοπούς αναφοράς και ελέγχου.

❖ **<u>Υπηρεσίες Microsoft Cloud</u>** Οι υπηρεσίες cloud της Microsoft λαμβάνουν αυστηρά μέτρα για να προστατεύσουν τα δεδομένα των πελατών των εταιρειών από ακατάλληλη πρόσβαση ή χρήση από μη εξουσιοδοτημένα άτομα. Αυτά τα μέτρα περιλαμβάνουν τον περιορισμό της πρόσβασης του προσωπικού της Microsoft και των υπεργολάβων και τον προσεκτικό καθορισμό των απαιτήσεων για την ανταπόκριση σε κυβερνητικά αιτήματα για δεδομένα πελατών. Το cloud της Microsoft είναι ειδικά σχεδιασμένο για να βοηθήσει να κατανοήσουν οι επιχειρήσεις τους κινδύνους και να τους αντιμετωπίσουν, και είναι σαφώς ασφαλέστερα από τα περιβάλλοντα υπολογιστών που βρίσκονται στο χώρο εργασίας. (Microsoft,: “Beginning your General Data Protection Regulation (GDPR) Journey-Accelerate GDPR compliance with the Microsoft Cloud”)

6.4 Οι εταιρείες ως σύμβουλος συμμόρφωσης για το GDPR

Πολλές εταιρείες στη χώρα μας, αναλύοντας σε βάθος τον νέο Κανονισμό, αποφάσισαν αντί να δημιουργήσουν εφαρμογές συμμόρφωσης με τον GDPR, να παρέχουν υπηρεσίες συμβούλου-εκπαιδευτή. Από τις 25 Μαΐου 2018, ημέρα καθολικής και υποχρεωτικής εφαρμογής του Κανονισμού, πολλές εταιρίες άρχισαν να δραστηριοποιούνται άμεσα προσπαθώντας καταρχήν να κατανοήσουν σε βάθος τις παραμέτρους του Κανονισμού, εγείροντας ερωτήματα και λύσεις. Στη συνέχεια, ξεκινούν την εφαρμογή αυτών των πρακτικών και την συμμόρφωση στις επιταγές του Κανονισμού στον δικό τους οργανισμό, με πρωταρχικό μέλημα την εκπαίδευση του προσωπικού τους, η οποία πραγματοποιείται σε τακτικά χρονικά διαστήματα. Με αυτό τον τρόπο δοκιμάζουν στην πράξη την εφαρμογή και τα αποτελέσματα του Κανονισμού, ώστε να μπορέσουν μετέπειτα να συνεισφέρουν στην περαιτέρω επιμόρφωση και των υπολοίπων που διατηρούν προσωπικά δεδομένα.

6.4.1 Σύμπραξη των εταιρειών «Alcosystems» και «Priority»

Μια περίπτωση εταιρειών που ένωσαν την τεχνογνωσία τους για την καλύτερη συμμόρφωση των πελατών τους προς τον νέο Κανονισμό, είναι αυτή των εταιρειών «Alcosystems» και «Priority».

Από τη μια η εταιρεία «Alcosystems», γνωστή στον επιχειρηματικό κόσμο για τις τεχνολογικές λύσεις και την κάλυψη αναγκών σχετικά με τα προσωπικά δεδομένα που προσφέρει στους πελάτες της, και από την άλλη η εταιρεία «Priority» που εξειδικεύεται από το 1995 στον τομέα της ανάλυσης και βελτίωσης των επιχειρησιακών διαδικασιών και ικανοποιεί απαιτήσεις κανονιστικής συμμόρφωσης αλλά και προσθέτει αξία στην επιχείρηση, ιδιαίτερα στον τομέα της διακυβέρνησης πληροφορικής, της ασφάλειας δεδομένων και της αξιολόγησης κινδύνων. Με τη συνεργασία μεταξύ Algosystems και Priority, επιτυγχάνεται η παροχή μιας συνολικής λύσης αναφορικά με τη συμμόρφωση στον GDPR, αφού η Priority αναλαμβάνει την εκπόνηση μελέτης για το εντοπισμό των σημείων που η εταιρεία βρίσκεται εκτεθειμένη έναντι του GDPR και η Algosystems προτείνει τεχνολογικές λύσεις κάλυψης των κενών που προέκυψαν από τη μελέτη και αναλαμβάνει την εκτέλεσή τους. Οι δύο εταιρείες προσφέρουν αυτό ακριβώς που οι πελάτες τους χρειάζονται για να προσεγγίσουν το GDPR με επιτυχία: πληρότητα, αξιοπιστία, λογική προσέγγιση

στα πλαίσια του εφικτού, ελάχιστη κατά το δυνατό διαταραχή στη τρέχουσα επιχειρησιακή δραστηριότητά τους, και εντέλει, προσφορά γνώσης και υπηρεσίας υψηλής προστιθέμενης αξίας επικεντρωμένης στην επίτευξη του στόχου για το οποίο έχουν κληθεί-τη συμμόρφωση του πελάτη τους με τον νέο κανονισμό GDPR.[17]

Αξίζει να σημειωθεί, πως παρόλο που οι δύο εταιρείες παρέχουν εξωτερικές υπηρεσίες DPO, εν τούτοις αρκετές φορές συμβουλεύουν τους πελάτες τους να εμπιστευτούν τον ρόλο σε δικό τους στέλεχος, που γνωρίζει πολύ καλά τις διαδικασίες της εταιρείας και μπορεί να κατανοήσει νομικά και τεχνολογικά θέματα., όπως χαρακτηριστικά αναφέρει σε συνέντευξή του στο περιοδικό "Netweek" ο κ. Αναστασάκης, CEO στην εταιρία Priority. (GDPR: Χρήσιμες Συμβουλές για όσες επιχειρήσεις δεν έχουν ξεκινήσει ακόμα, Ετήσια έκδοση 2017)

6.4.2 SYNTAX Πληροφορική A.B.E.E.

Ο όμιλος SYNTAX επικεντρώνεται στην ενεργοποίηση και την εξέλιξη της επιχειρηματικής δραστηριότητας των πελατών, συνδυάζοντας την τεχνολογία λογισμικού, παρέχοντας συμβουλευτικές υπηρεσίες, σχεδιασμό λύσεων, ενεργοποίηση, εξωτερική ανάθεση και διαχειριζόμενες υπηρεσίες. Με βάση την μακροχρόνια εμπειρία τους σε θέματα προστασίας της ιδιωτικότητας των πληροφοριών, έχουν επιλέξει τον σχεδιασμό ενός ολιστικού μοντέλου που εξασφαλίζει τη συμμόρφωση των οργανισμών με τον Κανονισμό και επιτρέπει τον αξιόπιστο επιχειρηματικό έλεγχο της πληροφορίας.

Στην παροχή υποστήριξης σχετικά με τον GDPR, επιδιώκει να συνεισφέρει στα προβλήματα που αντιμετωπίζουν οι οργανισμοί, καθώς οι περισσότεροι δεν γνωρίζουν τι πληροφορίες διατηρούν και ποιες από αυτές έχουν κάποια αξία, πού βρίσκονται τα ευαίσθητα δεδομένα, ούτε ποιος έχει πρόσβαση σε αυτά και όταν υπάρχει ανάγκη αναζήτησης, αυτή είναι ιδιαίτερα χρονοβόρα με τα αποτελέσματα να μην είναι πλήρη ούτε ορθά.

Το μοντέλο λοιπόν που εφαρμόζει ο όμιλος στους πελάτες της, βασίζεται σε τέσσερις πυλώνες που είναι ίδιοι με αυτούς που έχει ορίσει και η Microsoft:

[17] Πηγή: www.algosystems.gr «GDPR, ALGOSYSTEMS και PRIORITY. It's time to meet your GPDR Challenge!»

1) Ανακάλυψη (Discover), όπου "ανακαλύπτονται" τα δεδομένα του οργανισμού, αντιστοιχούνται σε ιδιοκτήτες και κατηγοριοποιούνται ανάλογα με την αξία τους και το βαθμό ευαισθησίας τους.

2) Προστασία (Protect), όπου υλοποιούνται μηχανισμοί προστασίας των δεδομένων τόσο αναφορικά με την διατήρηση της εμπιστευτικότητας και ακεραιότητας, όσο και από μη εξουσιοδοτημένη πρόσβαση.

3) Έλεγχος (Control), όπου υλοποιούνται μηχανισμοί ελέγχου της πρόσβασης στην πληροφορία και της αποτροπής διαρροών και μη ορθής χρήσης.

4) Αναζήτηση (Investigate), όπου υλοποιούνται μηχανισμοί παρακολούθησης των παραπάνω, καθώς και αναζήτησης πληροφοριών.

Τα παραπάνω στάδια, η υλοποίηση των οποίων αποτελεί συνδυασμό τεχνολογικών λύσεων και συμβουλευτικών υπηρεσιών, υλοποιούνται βασισμένα τόσο σε υπηρεσίες στρατηγικού σχεδιασμού και εξασφάλισης (assurance), όσο και παροχής υπηρεσιών Interim (Chief) Data Protection Officer.

Επιπλέον, η SYNTAX Πληροφορική, με την παραπάνω προσέγγιση δίνει στην οικονομική οντότητα, εκτός της δυνατότητας συμμόρφωσης με το νέο κανονιστικό πλαίσιο, τη δυνατότητα βέλτιστης αξιοποίησης της επιχειρησιακής πληροφορίας. Ουσιαστικά, προσφέρει στον οργανισμό τη δυνατότητα μεγιστοποίησης του ROI (Return on Information), σε αντιδιαστολή με το γνωστό Return on Investment.

Η μεγιστοποίηση της προσδοκώμενης αξίας των δεδομένων του οργανισμού επιτυγχάνεται μέσω της:

1) Ελαχιστοποίησης των φυσικών εγγραφών.

2) Ελαχιστοποίησης των διατηρούμενων δεδομένων, στο αναγκαίο για την υποστήριξη των επιχειρησιακών λειτουργιών και στόχων.

3) Δημιουργίας χρονοπρογραμματισμού διατήρησης των απαραίτητων δεδομένων σε συμμόρφωση με το κανονιστικό πλαίσιο.

4) Δημιουργίας ενός επιχειρησιακού σχεδίου κατηγοριοποίησης-ταξινόμησης των δεδομένων.

5) Ελαχιστοποίησης των κινδύνων κανονιστικής μη συμμόρφωσης. (Καλαντζής , Ετήσια έκδοση 2017)

6.4.3 Intracom Telecom

Η Intracom Telecom, ένας από τους κορυφαίους κατασκευαστές τηλεπικοινωνιακών συστημάτων και προμηθευτής ολοκληρωμένων λύσεων και επαγγελματικών υπηρεσιών για τηλεπικοινωνιακούς οργανισμούς σταθερής και κινητής, έχει δημιουργήσει μια έμπειρη και αποδοτική ομάδα εμπειρογνωμόνων, για την καλύτερη υποστήριξη των συνεργατών της στην ενσωμάτωση του GDPR. Η ομάδα της INTRACOM αποτελείται από:

1) Νομικούς εμπειρογνώμονες με σχετικό υπόβαθρο και μακρά εμπειρία στην προστασία προσωπικών δεδομένων.

2) Εμπειρογνώμονες διακυβέρνησης και συμμόρφωσης.

3) Εμπειρογνώμονες και Συμβούλους Πεδίου Ασφαλείας και Ευελιξίας Πληροφοριών.

4) Ειδικούς πληροφοριακών συστημάτων με σχετικό υπόβαθρο σε εφαρμογές, βάσεις δεδομένων, συστήματα, δίκτυα, επικοινωνίες και υποδομές.

5) Διαχειριστές προγραμμάτων και έργων σε επίπεδο εμπειρογνωμόνων με εξαιρετική εμπειρία.

Η προσέγγιση της Intracom για τον GDPR έχει ως σκοπό την ανακάλυψη προσωπικών δεδομένων, την κατηγοριοποίηση και την ταξινόμησή τους, την προστασία και την διασφάλιση της ιδιωτικότητάς τους. Πιο συγκεκριμένα, εφαρμόζει τις παρακάτω φάσεις στη διαδικασία συμμόρφωσης της εταιρείας με την οποία αναλαμβάνει να συνεργαστεί:

1) Έναρξη Έργου, Ομάδα & Δέσμευση: Καθορισμός των αναγκών του έργου σχετικά με το πεδίο εφαρμογής του, των στόχων, της έκτασης και των πόρων του (π.χ. προϋπολογισμός, ανθρώπινο δυναμικό, κ.λπ.). Δημιουργία ομάδας έργου, ευαισθητοποίηση και κατάρτιση των εργαζομένων.

2) Εκτέλεση χαρτογράφησης περιβάλλοντος: Κατανόηση των εννοιών των ελεγκτών, των επεξεργαστών και των προσωπικών δεδομένων. Προσδιορισμός όλων των ειδών επεξεργασμένων δεδομένων (μέσω συστημάτων πληροφορικής, διεργασιών κ.λπ.) και ανακάλυψη δεδομένων. Προσδιορισμός όλων των σχετικών ροών δεδομένων και πληροφοριών και των εφαρμόσιμων απαιτήσεων του GDPR.

3) Εκτέλεση ανάλυσης ελλείψεων (GAP Analysis): Προσδιορισμός της τρέχουσας κατάστασης έναντι των απαιτήσεων τους GDPR, λαμβάνοντας υπόψιν τους τύπους δεδομένων, τις πολιτικές και διαδικασίες που εφαρμόζονται, την επεξεργασία των δεδομένων από τρίτους και τις ροές εντός και εκτός της ΕΕ.

4) Προσδιορισμός των κινδύνων και αξιολόγηση των επιπτώσεων τους στην ιδιωτική ζωή (DPIA): Ανάλυση των πιθανών κινδύνων και καθορισμός των επιπτώσεων και των αποτελεσμάτων της συλλογής, συντήρησης, χρήσης και διάδοσης των προσωπικών δεδομένων σύμφωνα με τις απαιτήσεις του GDPR. Προσδιορισμός και αξιολόγηση των υφιστάμενων ελέγχων και διαδικασιών (τόσο τεχνικών όσο και οργανωτικών).

5) Πρόταση σχεδίου για περιορισμό των κινδύνων και συμμόρφωση: Καθορισμός του οδικού χάρτη πορείας (Roadmap) και πρόταση σχεδίου εφαρμογής για τον περιορισμό των δυνητικών κινδύνων στην προστασία της ιδιωτικής ζωής και της ασφάλειας.

6) Αρχιτεκτονική και σχεδιασμός πλαισίου: Πλάνο σχεδιασμού με αμοιβαία συμφωνημένα μέτρα (έλεγχοι / διαδικασίες τόσο τεχνικές όσο και οργανωτικές) για την αντιμετώπιση πιθανών κινδύνων για την ιδιωτικότητα και την ασφάλεια.

7) Παράδοση υλοποίησης: Μέτρα και τεχνικές εκτέλεσης της υλοποίησης και των ελέγχων για τον περιορισμό των δυνητικών κινδύνων στην προστασία της ιδιωτικότητας.

8) Επιβεβαίωση συμμόρφωσης διακυβέρνησης, Παρακολούθηση & Υποστήριξη: Αναθεώρηση GAP ανάλυσης, έλεγχος λειτουργίας συστήματος παρακολούθησης και διαχείρισης. Παροχή υποστήριξης και συμβουλευτικών υπηρεσιών για την εταιρεία. (Vordos, 2017)

6.5 Σύνοψη

Στο συγκεκριμένο κεφάλαιο, περιγράφηκαν μερικά από τα πιο γνωστά πληροφοριακά συστήματα που δημιουργήθηκαν από τις μεγάλες εταιρίες hardware και software σχετικά με την ομαλή συμμόρφωση των οικονομικών οντοτήτων με τον GDPR. Η εναρμόνιση αυτή επιτυγχάνεται χάρις στα εργαλεία που έχουν αναπτύξει οι εταιρείες, καθώς και στην ουσιαστική συνεισφορά κάποιων άλλων εξωτερικών εταιρειών, κυρίως ελληνικών στην παροχή υπηρεσιών συμμόρφωσης με τον GDPR και εκπαίδευσης του ανθρωπίνου δυναμικού.

Είναι φανερό πως η είσοδος στην επαγγελματική καθημερινότητα των οικονομικών οντοτήτων, του νέου Κανονισμού έχει οδηγήσει αρκετές εταιρείες στο να εκμεταλλευτούν το γεγονός αυτό, παρέχοντας και σχεδιάζοντας νέα εξειδικευμένα συστήματα ή αναβαθμίζοντας τα ήδη υπάρχοντα με τη προσθήκη νέων εργαλείων προσαρμοσμένων στον νέο Κανονισμό. Δίνεται η δυνατότητα ωστόσο στις μεγάλες κυρίως εταιρείες να προμηθευτούν την εφαρμογή που ταιριάζει καλύτερα στην υλοποίηση της στρατηγικής της για την αποτελεσματική συμμόρφωση με τον GDPR, γιατί τόσο το κόστος εγκατάστασης όσο και συντήρησης αυτών των εφαρμογών είναι αρκετά υψηλό. Ο νέος Κανονισμός, ορίζει πλέον μια νέα πραγματικότητα όσον αφορά τις οικονομικές οντότητες ιδιωτικές ή δημόσιες και τα προσωπικά δεδομένα, και οι εταιρίες λογισμικών εγχώριες ή εξωχώριες, αποτελούν τους αρωγούς ως προς την σωστή και ομαλή συμμόρφωση και εναρμόνιση με τον GDPR.

ΜΕΡΟΣ Β: ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

ΚΕΦΑΛΑΙΟ7 :ΜΕΛΕΤΗ ΠΕΡΙΠΩΣΕΩΝ ΕΦΑΡΜΟΓΗ ΜΕΘΟΔΟΛΟΓΙΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΣΕ ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΚΑΙ ΣΕ ΕΛΛΗΝΙΚΗ ΤΡΑΠΕΖΑ

7.1 Εισαγωγή

Στο παρόν κεφάλαιο, που αποτελεί και των πυρήνα της παρούσης διπλωματικής εργασίας, γίνεται μια προσπάθεια σύνδεσης και αξιοποίησης όλων των προηγούμενων στοιχείων σχετικά με το θεωρητικό υπόβαθρο του νέου Κανονισμού, εφαρμοσμένα στην ελληνική πραγματικότητα. Από στοιχεία που αντλήθηκαν από το διαδίκτυο, καθώς και από στοιχεία που προήλθαν μετά από έρευνα μελετάτε η πρακτική εφαρμογή της μεθοδολογίας συμμόρφωσης με τον GDPR τόσο από μία φαρμακευτική ελληνική ιδιωτική εταιρία, όσο και από μία εγχώρια συστημική Τράπεζα, δύο κλάδοι που επηρεάζονται άμεσα από τις νέες διατάξεις του Κανονισμού.

Αξίζει να σημειωθεί πως για τα παρακάτω στοιχεία που θα παρουσιαστούν, έχουν γίνει όλες οι απαραίτητες ενέργειες και έχει ληφθεί η απαραίτητη άδεια χρησιμοποίησης τους από τους ιθύνοντες. Τα στοιχεία που παρουσιάζονται παρακάτω, είναι αποτέλεσμα έρευνας και προσωπικής επικοινωνία με τους ιθύνοντες των οικονομικών οντοτήτων. Και σε αυτό το σημείο θα ήθελα και πάλι να ευχαριστήσω τον κ. Ευαγγελίδη Αντώνιο, για την αμέριστη βοήθεια που μου παρείχε. Είναι σημαντικό να αναφερθεί πως για λόγους ανταγωνισμού αλλά και απορρήτου, μας ζητήθηκε η χρησιμοποίηση των στοιχείων, να γίνει ανώνυμα και να μην αναφερθεί ούτε το όνομα της Τράπεζας, ούτε το όνομα της ελληνικής φαρμακευτικής εταιρείας.

7.2 Εφαρμογή του GDPR σε μια ελληνική φαρμακευτική εταιρεία

Η μετακίνηση δεδομένων ήταν πάντα μια περίπλοκη διαδικασία για τον κλάδο της υγείας, και για τις εταιρείες που δραστηριοποιούνται σε αυτόν, είτε δημόσιες είτε ιδιωτικές, όπως εταιρείες ιατρικού και φαρμακευτικού ενδιαφέροντος. Με την

εισαγωγή του GDPR, τίθεται το ερώτημα πώς οι επιχειρήσεις που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση θα συνεχίσουν να διεξάγουν δοκιμές, αφού ο νέος Κανονισμός θα δυσχεραίνει τις επιχειρήσεις να αποκτήσουν τα απαιτούμενα δεδομένα και να τα μοιραστούν με τους ερευνητές που πρέπει να τα ερμηνεύσουν. Οι πάροχοι υπηρεσιών υγείας, πρέπει να διασφαλίζουν ότι συμμορφώνονται με τις απαιτήσεις των δημόσιων αρχών και είναι σε θέση να αποδείξουν ότι προστατεύουν επαρκώς τις πληροφορίες των πελατών τους. με την δημιουργία ενός συστήματος που επιτρέπει τη διαγραφή ή τη διόρθωση των δεδομένων τους.

Η εν λόγω οικονομική οντότητα που αποτελεί και το αντικείμενο της έρευνας σχετικά με την συμμόρφωση με τον Κανονισμό, είναι μια ελληνική φαρμακευτική εταιρεία με ετήσιες πωλήσεις που αγγίζουν τα 300.000.000€. Η οργανωτική δομή της εταιρείας, αποτελείται από 4 εργοστάσια παραγωγής που όλα εδρεύουν στην Ελλάδα, καθώς και από 8 περιφερειακά γραφεία, ενώ στις τάξεις της απασχολούνται περισσότεροι από 1000 υπάλληλοι. Το πελατολόγιό της αποτελείται από πελάτες τόσο στο εσωτερικό, όσο και στο εξωτερικό, με εξαγωγές σε 37 χώρες του κόσμου και με συνεργασία με τους μεγαλύτερους φαρμακευτικούς ομίλους παγκοσμίως.

Όπως αναφέρει χαρακτηριστικά ο κ. Ευαγγελίδης στην εκδήλωση σχετικά με το GDPR που οργάνωσε η TÜV AUSTRIA HELLAS, «στον κλάδο της φαρμακευτικής υπάρχουν πολυεθνικές εταιρείες όπου η «εμπειρία στο GDPR, βασίζεται στην εμπειρία που έχουν οι μητρικές εταιρείες και προσπαθούν να διαβιβάσουν στις θυγατρικές. Στην ενασχόληση όμως με την υλοποίηση του GDPR, σε ελληνική φαρμακευτική εταιρεία, έχεις να αντιμετωπίσεις κάποιες προκλήσεις- προβλήματα. Αρχικά ξεκινάς από το μηδέν, πρέπει να στήσεις όλο το πρόγραμμα και όλους τους συντελεστές χωρίς βοήθεια παρότι την χρειάζεσαι αλλά δεν την έχεις από την πρώτη στιγμή».

Η μόνη λύση λοιπόν που σου απομένει, είναι η κατανόηση των νέων δεδομένων που φέρνει ο Κανονισμός καθώς και της σημασίας του, βλέποντάς το ως «λανσάρισμα» ενός νέου φαρμακευτικού προϊόντος. Αυτό το προϊόν απαιτεί μια πανευρωπαϊκή έγκριση, η οποία σε περίπτωση που δεν αποδοθεί σωστά θα της κοστίσει την επιβολή προστίμου που κυμαίνεται στο 4% του ετήσιου τζίρου της, ήτοι 20.000.000€. Η ημερομηνία εισαγωγής του φαρμακευτικού αυτού προϊόντος ορίζεται

η 25η Μαΐου 2018, ενώ χαριτολογώντας ονόμασε τον Κανονισμό GDPR ως φάρμακο «Privacin» 15 αόρατες κάψουλες που εξασφαλίζουν την ιδιωτικότητά του.

7.2.1 Οδικός Χάρτης Προετοιμασίας του GDPR από μια ελληνική φαρμακευτική εταιρεία

Το πρώτο βήμα της υλοποίησης του GDPR, ξεκίνησε με τη δημιουργία ενός οδικού χάρτη σε μορφή πυραμίδας, που βοήθησε τη φαρμακευτική εταιρία να οργανωθεί καλύτερα.

Στο πρώτο στάδιο η εταιρεία διαμόρφωσε τη στρατηγική της για την προετοιμασία και τη συμμόρφωσή της με τον GDPR. Σε αυτό το στάδιο έπρεπε να διαμορφώσει το όραμα και την αποστολή της, ώστε να εξασφαλίζονται οι ανάγκες των πελατών της, εσωτερικών και εξωτερικών.

Στη συνέχεια, έπρεπε να λάβει υπόψιν της την οργάνωση και τη «λογοδοσία» στο εσωτερικό κομμάτι της επιχείρησης και μετέπειτα να εξασφαλίσει όλα εκείνα τα μέτρα που θα δημιουργούσαν την αναγκαία οργανωτική και επιχειρησιακή κουλτούρα εντός της επιχείρησης, μέσω της κατάλληλης επικοινωνίας, εκπαίδευσης και κινητοποίησης των στελεχών και εργαζομένων της.

Στο επόμενο στάδιο, συγκρότησε τα διάφορα βήματα, τις πολιτικές, και τις διαδικασίες-παρεμβάσεις που θα έπρεπε να κάνει για τη διαχείριση και μεταφορά των προσωπικών δεδομένων, ώστε να μπορέσει να περάσει στο στάδιο της αντιμετώπισης των διαφόρων παρεμβάσεων της ιδιωτικότητας, με σημαντικότερη την εκτίμηση των επιπτώσεων της προστασίας των δεδομένων (DPIA).

Στο τελικό στάδιο, αφού εξασφαλίσει τα απαραίτητα πληροφοριακά συστήματα και λογισμικά υποστήριξης, θα μπορέσει να κάνει την επεξεργασία και την απογραφή των δεδομένων που χρειάζεται (inventority).

Εικόνα 13: Οδικός Χάρτης Ετοιμότητας της ελληνικής φαρμακευτικής εταιρείας με τον GDPR

Έχοντας έτσι κατά νου το παραπάνω διάγραμμα, και θέτοντας διάφορους στόχους και οράματα, και μελετώντας διάφορες περιπτώσεις (case studies), οι υπεύθυνοι κατέληξαν στο ακόλουθο όραμα για τους πελάτες της:

- ✓ Σεβασμός του θεμελιώδους δικαιώματος της ιδιωτικότητάς τους.
- ✓ Πραγματοποίηση όλων των αναγκαίων διασφαλίσεων για την προστασία της ασφάλειας και της εμπιστευτικότητας των προσωπικών δεδομένων που συγκεντρώνονται, χρησιμοποιούνται ή δημοσιοποιούνται στο πλαίσιο των αλληλεπιδράσεων.
- ✓ Περιορισμός των προσωπικών δεδομένων που συγκεντρώνονται στο ελάχιστο δυνατόν, προκειμένου να προσφέρονται καλύτερες υπηρεσίες.
- ✓ Άδεια μόνο σε κατάλληλα εκπαιδευμένο, εξουσιοδοτημένο προσωπικό να έχει πρόσβαση σε αυτά.
- ✓ Να μη δημοσιοποιούνται τα προσωπικά τους δεδομένα σε εξωτερικά μέρη, εκτός αν συναινούν οι ίδιοι οι πελάτες ή έχουν προηγουμένως πληροφορηθεί από την εταιρεία ή απαιτείται εκ του νόμου.

7.2.3 Φάσεις έργου συμμόρφωσης με τον GDPR

Με την ολοκλήρωση της αποδοχής ενός κοινού οράματος για όλο το ανθρώπινο

δυναμικό της εταιρείας, σχεδιάστηκαν και οι φάσεις του έργου για τη συμμόρφωση με τον GDPR.

Οι φάσεις αυτές, όπως φαίνονται και στο παρακάτω διάγραμμα, χωρίζονται:

1) Στην **1η φάση**, της προετοιμασίας και της οργάνωσης της εταιρίας για την ενσωμάτωση του Κανονισμού όπου μελετάται η Νομοθεσία και κατανοούνται οι οδηγίες του GDPR. Στη συγκεκριμένη φάση, που πραγματοποιήθηκε την περυσινή χρονιά, το κόστος ανήλθε γύρω στα 34.000€, αν συνυπολογισθούν και οι εκπαιδεύσεις που πραγματοποιήθηκαν, οι ενέργειες ευαισθητοποίησης, τα συνέδρια και οι διάφορες εκδηλώσεις που πραγματοποιήθηκαν, κ.α.

2) Στη **2η φάση**, της αξιολόγησης-εκτίμησης των επιπτώσεων και της διάγνωσης των τομέων που χρήζουν αλλαγών για την ομαλή μετάβαση στον GDPR (Assessment). Στη συγκεκριμένη φάση, βρίσκεται αυτήν την στιγμή η εταιρία, η οποία φτάνει στο τέλος της οσονούπω. Το κόστος της υλοποίησης με διάφορες ενέργειες που πραγματοποιήθηκαν, όπως εκτυπώσεις υλικών κ.α. ανέρχεται στα 80.000€.

3) Στην **3η φάση**, που είναι η υλοποίηση του στρατηγικού πλάνου και σχεδίου προετοιμασίας, με σκοπό την ετοιμότητα για εφαρμογή του GDPR στην προστασία των δεδομένων (Implementation).

Συνολικά λοιπόν, το κόστος για την συμμόρφωση με τον GDPR από την εν λόγω οικονομική οντότητα, ανέρχεται σε 100.000€ χωρίς να συνυπολογίζεται σε αυτό το τρίτο κομμάτι, που έχει να κάνει με το κομμάτι των οργανωτικών και τεχνολογικών μέτρων που θα αγοράσει η εταιρεία, και έχει να κάνει κυρίως με εφαρμογές και προγράμματα υπολογιστών που θα δημιουργήσουν τεχνικές ανωνυμοποίησης και ψευδωνυμοποίησης, κρυπτογράφησης κ.α. Ακόμη θα χρειαστούν μηχανές για καταστροφή εγγράφων (shredder), ταμπέλες, υπεύθυνοι προστασίας, και άλλες ενέργειες οι οποίες εκτιμώνται πως θα αγγίξουν τις 50.000-70.000€. Όπως χαρακτηριστικά αναφέρει ο κ. Ευαγγελίδης σε αντίστοιχη ερώτηση που του τέθηκε, το κόστος θα μπορούσε να είναι πολύ υψηλότερο, όμως προσπάθησαν το κόστος να είναι προσαρμοσμένο στην ελληνική πραγματικότητα λαμβάνοντας υπόψιν και την οικονομική κρίση, αλλά και το μέγεθος της εταιρίας. Διαφορετικά διαχειρίζεται ένα αντίστοιχο πρόγραμμα μια ελληνική εταιρεία που αποτελεί μέρος μιας πολυεθνικής μεγαλύτερης εταιρείας που εδρεύει στην Αμερική ή την Ευρώπη, και διαφορετικά

από μια ελληνική κατά κόρον εταιρεία. Οι εταιρείες που αποτελούν μέρος μιας πολυεθνικής εταιρείας, βασίζονται στο ότι έχει ετοιμάσει η «μητρική» εταιρεία, σε πολιτικές, διαδικασίες, συστήματα, εφαρμογές τα οποία υποχρεωτικά πρέπει να ακολουθήσουν και να εφαρμόσουν. Αντίθετα μια εταιρεία, όπως η εξετάζουσα η οποία έχε τον ρόλο και της μητρικής και της θυγατρικής, ξεκινάει από το μηδέν και χωρίς καμία βοήθεια την προσπάθεια αρχικά κατανόησης του Κανονισμού και στη συνέχεια την προσπάθεια συμμόρφωσης.

Εικόνα 14: Φάσεις έργου συμμόρφωσης με τον GDPR

Έτσι σημαντικό και πρωταρχικής σημασίας η φαρμακευτική εταιρία και ο ίδιος ο DPO έδωσαν στο να δεσμευτούν οι ιθύνοντες της εταιρίας και τα ανώτατα στελέχη της, στο να γνωρίσουν και να στηρίξουν το GDPR, ούτως ώστε να επιτευχθεί η εύρυθμη εφαρμογή του και να μην ζητηθούν ευθύνες μόνο από τον υπεύθυνο της προστασίας δεδομένων DPO. Ακόμη η εταιρεία κατέληξε στο συμπέρασμα, πως ο GDPR δεν μπορεί να εφαρμοστεί από ένα μόνο πρόσωπο, αλλά από μια ομάδα ανθρώπων ώστε να βοηθήσει ο ένας τον άλλο. Έτσι κατέληξαν στο ότι χρειάζονται και οικονομικοί και ανθρώπινοι πόροι. Αναλυτικότερα:

1) Πρώτη φάση: Προετοιμασία και Οργάνωση

- <u>Δημιουργία Ομάδας Έργου και DPO</u>

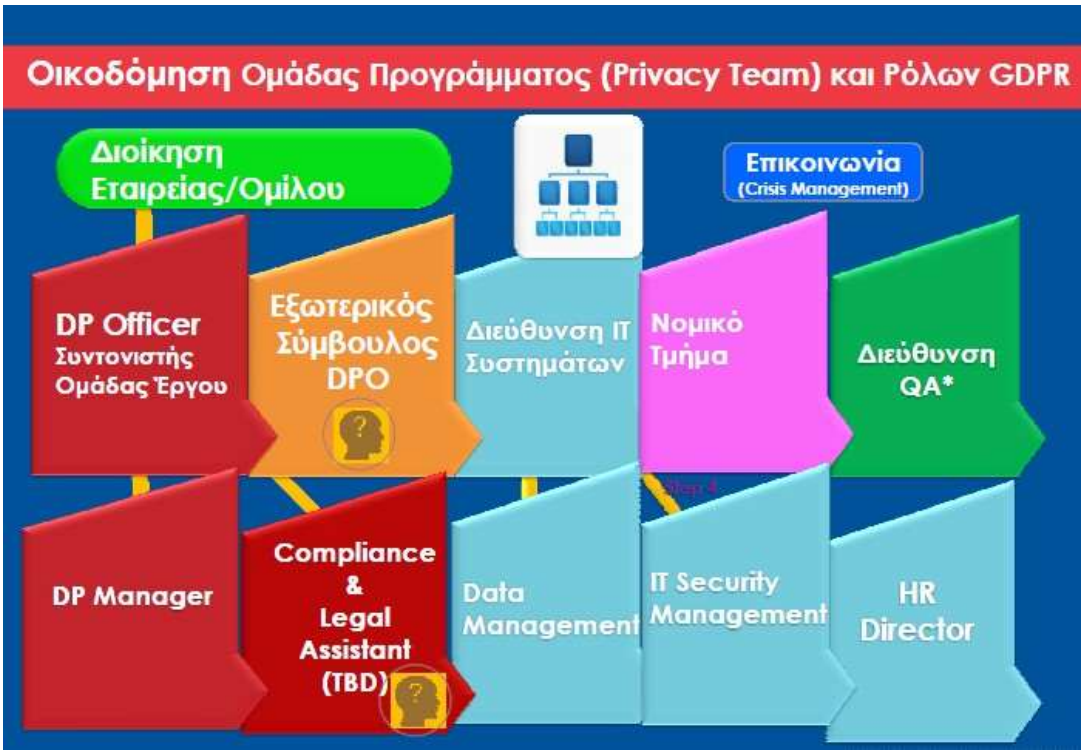
Στη συγκεκριμένη φάση, απαιτείται η δέσμευση και η στήριξη της Διοίκησης και των Ανώτατων Στελεχών για την εκπλήρωση του έργου, διότι χωρίς αυτά, ό,τι αλλαγή και προσπάθεια να γίνει στην εταιρεία, δεν θα έχει αποτέλεσμα. Η Ανώτατη Διοίκηση οφείλει να κατανοήσει ότι είναι υπεύθυνη για τη λογοδοσία και για την εξασφάλιση και έγκριση των απαραίτητων πόρων (ανθρώπινων, υλικών, τεχνολογικών, χρόνου κλπ.) που θα συμμετέχουν στην υλοποίηση του έργου.

Επιπλέον, καθορίζονται οι ευθύνες και οι αρμοδιότητες για κάθε μέλος της εταιρείας. Ορίζεται υποχρεωτικά ο Υπεύθυνος Προστασίας των Δεδομένων (DPO) και η ομάδα υποστήριξης του προγράμματος και δημιουργούνται ενδοτμηματικά οι σύνδεσμοι και οι «Πρεσβευτές» για την παρακολούθηση και συγκρότηση του έργου.

Η εν λόγω εταιρεία, έχει δημιουργήσει την ομάδα έργου της (Privacy Team) με βάση το διάγραμμα που ακολουθεί. Σε αυτό φαίνεται ότι συμμετέχουν, τόσο η Διοίκηση της εταιρείας και του ομίλου, όσο και:

- Ο εσωτερικός Υπεύθυνος Προστασίας Δεδομένων (DPO) που είναι και ο συντονιστής του έργου.
- Ο Διαχειριστής των δεδομένων (DP Manager).
- Ο εξωτερικός Υπεύθυνος Προστασίας Δεδομένων (DPO) που παρακολουθεί την όλη διαδικασία και παρέχει συμβουλές σχετικά με την πορεία και εξέλιξή της.
- Ο βοηθός συμμόρφωσης και παροχής νομικών υπηρεσιών (TBD).
- Η διεύθυνση των πληροφοριακών συστημάτων και λογισμικών.
- Το τμήμα διαχείρισης των δεδομένων.
- Το τμήμα διασφάλισης και προστασίας των πληροφοριακών συστημάτων.
- Το νομικό τμήμα, για την διευκόλυνση ερμηνείας των όρων και κανόνων του GDPR.
- Διευθυντής Ανθρώπινου Δυναμικού.
- Η Διεύθυνση Διασφάλισης Ποιότητας (Quality Assurance), η οποία έχει ως στόχο το συνεχή έλεγχο για τη διασφάλιση της τήρησης των κανόνων του έργου και τη συνεχή πιστοποίηση του σε συνεργασία με τον DPO, και τέλος
- Ο υπεύθυνος επικοινωνίας, για την ενημέρωση της κοινής γνώμης σε περίπτωση διαχείρισης κρίσεων από τυχόν διώξεις πελατών ως προς την εταιρεία ή κυρώσεων της Αρχής Προστασίας Δεδομένων. Για την αντιμετώπιση τέτοιων

περιστατικών, η εν λόγω οντότητα διοργανώνει σεμινάρια διαχείρισης κρίσεων για το προσωπικό της, ώστε να είναι έτοιμο με την ισχύ του GDPR.



Εικόνα 15: Δημιουργία Ομάδας Έργου GDPR από την ελληνική φαρμακευτική εταιρεία

- <u>Κατανομή ρόλων και αρμοδιοτήτων στην Ομάδα Έργου GDPR</u>

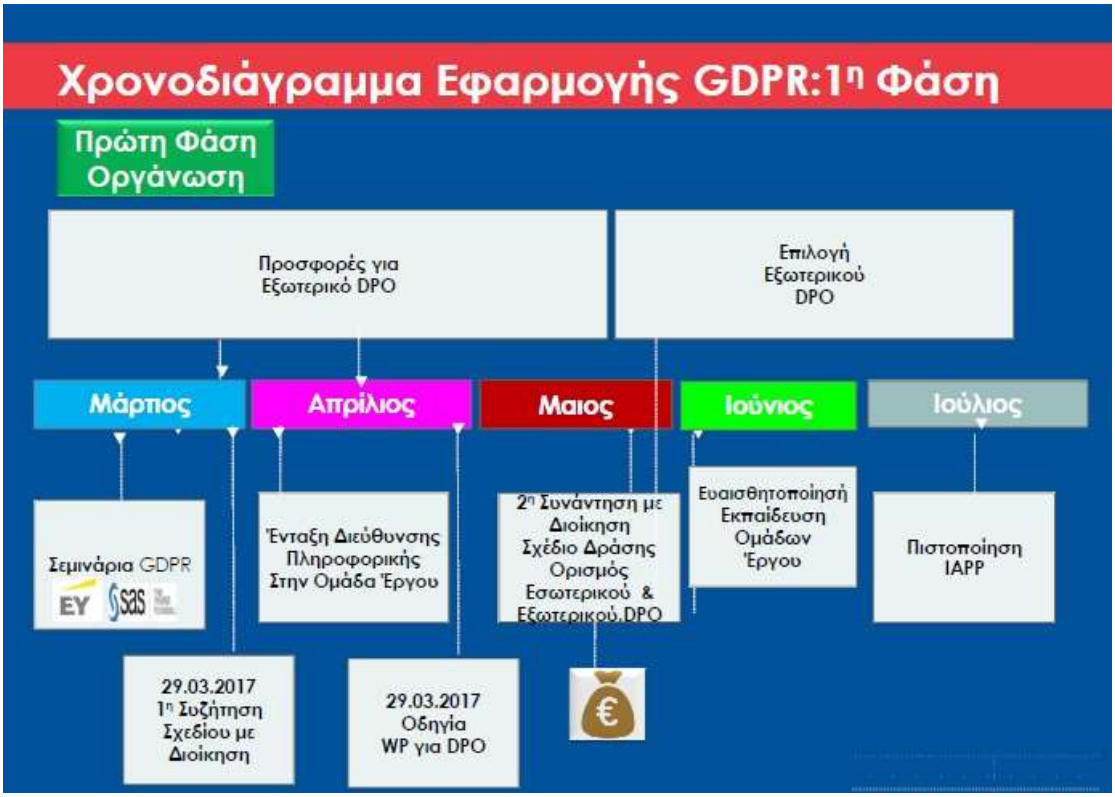
Στη διάρκεια της πρώτης φάσης του έργου συμμόρφωσης με τον GDPR, η εταιρεία κατανέμει ανά τακτά χρονικά διαστήματα τις σημαντικότερες αρμοδιότητες που πρέπει να διεκπεραιώσει η ομάδα έργου (Privacy Team), που αφορούν:

- Τις διαδικασίες, τις πολιτικές και την οργάνωση του έργου.
- Τη συνεχή ενημέρωση του ανθρώπινου δυναμικού και την εκπαίδευσή του.
- Την ανταπόκριση και την ετοιμότητα του προσωπικού σε έκτακτα συμβάντα.
- Το σχεδιασμό και την εκτέλεση των ελέγχων απορρήτου.
- Τον έλεγχο απορρήτου για υπάρχοντα προϊόντα και υπηρεσίες.
- Την εκτέλεση εκτίμησης επιπτώσεων για την προστασία των δεδομένων (DPIA).

- <u>Αλλαγή Κουλτούρας</u>

Το σημαντικότερο ωστόσο σημείο στη διάρκεια του έργου είναι η αλλαγή κουλτούρας, η αλλαγή νοοτροπίας των εργαζομένων και η δημιουργία ενός «ανθεκτικού» περιβάλλοντος, όπου θα εργάζονται όλοι για τον ίδιο σκοπό. Αν δεν υπάρχει η διαμόρφωση κουλτούρας στηριζόμενη σε ισχυρές βάσεις, τότε ο ρόλος του DPO και ο ρόλος του GDPR γενικότερα, δεν θα έχει καμία αξία και η εταιρεία θα είναι πλέον ιδιαίτερα ευάλωτη και εκτεθειμένη απέναντι σε ανεπιθύμητες ενέργειες και παραβιάσεις ή γραφειοκρατικούς κινδύνους.

Για την κινητοποίηση των εργαζομένων και τον ενστερνισμό μιας ενιαίας κουλτούρας, η εταιρεία δημιούργησε μια διεταιρική ομάδα 35 υψηλόβαθμων ατόμων από διάφορα τμήματα, των Πρεσβευτών (Ambassadors), τα οποία ενημερώνονται συνεχώς για τις εξελίξεις γύρω από το νέο Κανονισμό και αναλαμβάνουν την ενημέρωση σε όλα σχεδόν τα σημαντικά τμήματα της εταιρείας, υψηλού κινδύνου. Αυτό έχει σαν αποτέλεσμα να υπάρχει μεγάλη «ευαισθησία» και κινητικότητα μεταξύ των εργαζομένων για την εφαρμογή του GDPR και για τα προγράμματα ενημέρωσης σχετικά με αυτό.



Εικόνα 16: Χρονοδιάγραμμα 1ης φάσης GDPR στην ελληνική φαρμακευτική εταιρεία

2) Δεύτερη Φάση: Αξιολόγηση ετοιμότητας GDPR (Assessment)

Σε αυτή τη φάση, πραγματοποιείται μια σειρά ελέγχων, αξιολογήσεων και συνεντεύξεων, με σκοπό την καλύτερη δυνατή αποτύπωση της υφιστάμενης κατάστασης της επιχείρησης, των συστημάτων και των δεδομένων.

- Διάγνωση 360°- Χαρτογράφηση (Data Mapping)

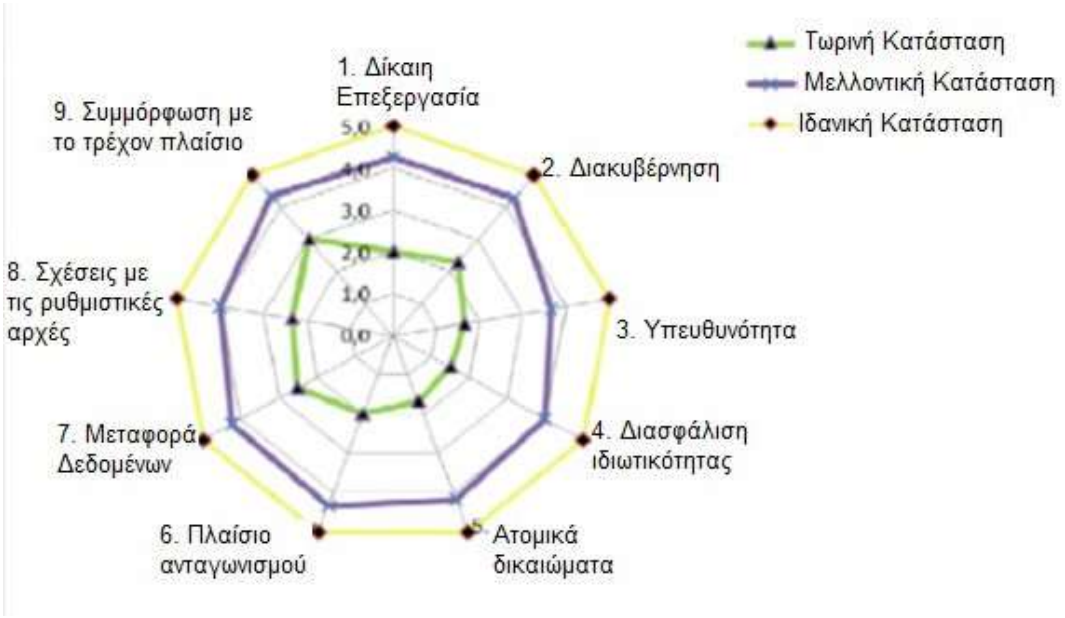
Η διάγνωση και χαρτογράφηση των δεδομένων πραγματοποιείται μέσω συνεντεύξεων, ερωτηματολογίων και workshops με πρώτης και δεύτερης βαθμίδας managers και αρμόδιων στελεχών. Σκοπός αυτής της πρακτικής ήταν να διαπιστώσει η εταιρεία ποια προσωπικά δεδομένα διαθέτει και σε ποιους ανήκουν, πώς συλλέγονται τα δεδομένα, πού και πώς μεταφέρονται (εντός και εκτός εταιρείας και ΕΕ), πού αποθηκεύονται, με χρήση ποιων λογισμικών και μέσων αποθήκευσης, με ποιους τρόπους επεξεργάζονται και πόσος χρόνος χρειάζεται για τη διαγραφή τους.

Με την ολοκλήρωση της συγκέντρωσης όλων των παραπάνω στοιχείων, δημιουργείται ο χάρτης της ροής δεδομένων (Data flow mapping), η ανάλυση ελλείψεων ως προς τον GDPR (Gap Analysis) και η εκτίμηση επιπτώσεων των προσωπικών δεδομένων (Privacy Impact Assessment-DPIA). Να σημειωθεί πως η διαδικασία των συνεντεύξεων δεν πραγματοποιήθηκε από άτομα της εταιρείας, αλλά από μια συμβουλευτική άλλη εταιρία που προσελήφθη, ούτως ώστε οι συνεντευξιαζόμενοι να είναι πιο χαλαροί χωρίς κάποιο φόβο, ώστε να ειπωθούν πραγματικότητες που θα βοηθήσουν στην πιο ουσιαστικότερη και πιο πετυχημένη χαρτογράφηση του GDPR.

- Αξιολόγηση Βαθμού ετοιμότητας (GDPR Readiness)

Στη συνέχεια, αξιολογείται ο βαθμός ετοιμότητας της φαρμακοβιομηχανίας, δηλαδή με βάση συγκεκριμένα παραδείγματα συγκρίνεται η κατάσταση στην οποία βρίσκεται η εταιρεία τώρα σε σχέση με την ιδεατή κατάσταση που θέλει να φτάσει.

Η εταιρεία συγκεκριμένα δημιούργησε ένα προφίλ ετοιμότητας GDPR (GDPR Maturity Profiile), αξιολογώντας την ετοιμότητά της στις εξής, ίσης βαρύτητας διαστάσεις, όπως φαίνεται στο παρακάτω σχήμα:



Εικόνα 17: GDRR Maturity Profile - Αξιολόγηση Βαθμού ετοιμότητας της ελληνικής φαρμακευτικής εταιρείας

Όπως διαπιστώνεται η παρούσα κατάσταση της εταιρείας απέχει ακόμα πολύ από τη μελλοντική κατάσταση και ακόμα περισσότερο από την ιδεατή κατάσταση στην οποία στοχεύει.

- <u>Ροή Δεδομένων-Πληροφοριών (Data/Information Flow)</u>

Ακολούθως, κατηγοριοποιούνται τα δεδομένα και οι πληροφορίες που υπάρχουν, προσδιορίζοντας τα σημεία κλειδιά όπως:

- Στοιχεία δεδομένων (π.χ. ονόματα, e-mails, διευθύνσεις – δεδομένα υγείας και ποινικά δεδομένα – βιομετρικά δεδομένα θέσης)
- Μορφές δεδομένων (π.χ. σε χαρτί, σε ψηφιακή μορφή, σε βάσεις δεδομένων)
- Μέθοδοι μεταφοράς δεδομένων (π.χ. μέσω ταχυδρομείου, τηλεφώνου, μέσων κοινωνικής δικτύωσης – ενδοεταιρικά – εξωτερικά)
- Τοποθεσίες δεδομένων (π.χ σε γραφεία, σε σύννεφα (clouds), σε τρίτα μέρη (third parties)

Με αυτόν τον τρόπο η εταιρεία αποκτά μια πλήρη εικόνα σχετικά με τη «διαδρομή» των δεδομένων εντός και εκτός της εταιρείας.

- Ανάλυση Ελλείψεων (Gap Analysis) ως προς τον GDPR

Αφού συλλέχτηκαν όλα τα παραπάνω στοιχεία, εφαρμόζεται η ανάλυση ελλείψεων για να διαπιστωθεί ποια είναι η παρούσα κατάσταση στην οποία βρίσκεται η εταιρεία, καθώς και τι ενέργειες απαιτούνται να γίνουν για να επιτευχθεί η πρόκληση ή ο στόχος που έχει θέσει η εταιρεία.

Τα ερωτήματα που τίθενται για να διαπιστωθούν τα σημεία που χρήζουν περαιτέρω προσοχής είναι αν:

- Επιτυγχάνονται οι βασικές αρχές προστασίας προσωπικών δεδομένων;
- Εξασφαλίζονται τα δικαιώματα των φυσικών προσώπων;
- Προβλέπεται η γνωστοποίηση παραβίασης προσωπικών δεδομένων;
- Είναι ασφαλής οι πληροφορίες;
- Είναι αποτελεσματική η οργανωτική δομή;
- Εφαρμόζονται οι πολιτικές και οι διαδικασίες όπως ορίστηκαν στο στρατηγικό πλάνο;
- Προβλέπονται συνεχείς επιθεωρήσεις και βελτιώσεις στην εφαρμογή του GDPR;

- Σχεδιασμός Προγράμματος Προστασίας Προσωπικών Δεδομένων (Compliance Plan) – Εξασφάλιση Δικαιωμάτων Φυσικών Προσώπων

Από την Ανάλυση Ελλείψεων (Gap Analysis) που πραγματοποίησε η εταιρεία και τις διαπιστώσεις που έκανε, διαμόρφωσε το πρόγραμμα συμμόρφωσης που περιλαμβάνει:

1) Την **αλλαγή πρακτικών** (π.χ. πληροφόρηση των πελατών, απαίτηση συναίνεσής τους στην επεξεργασία των δεδομένων τους, ελαχιστοποίηση του απαιτούμενου χρόνου διαγραφής των δεδομένων, ανωνυμοποίηση αυτών, αυστηρότεροι έλεγχοι πρόσβασης, σύναψη συμβάσεων με συνεργάτες και υπεύθυνους επεξεργασίας, θέσπιση αυστηρότερων πρακτικών ασφαλείας, κ.λπ.)

2) Τη **θέσπιση νέων μηχανισμών** (π.χ. για την εξασφάλιση των δικαιωμάτων των φυσικών προσώπων, για την αποτελεσματικότερη παρακολούθηση, βελτίωση και έλεγχο των προσωπικών δεδομένων, κ.λπ.),

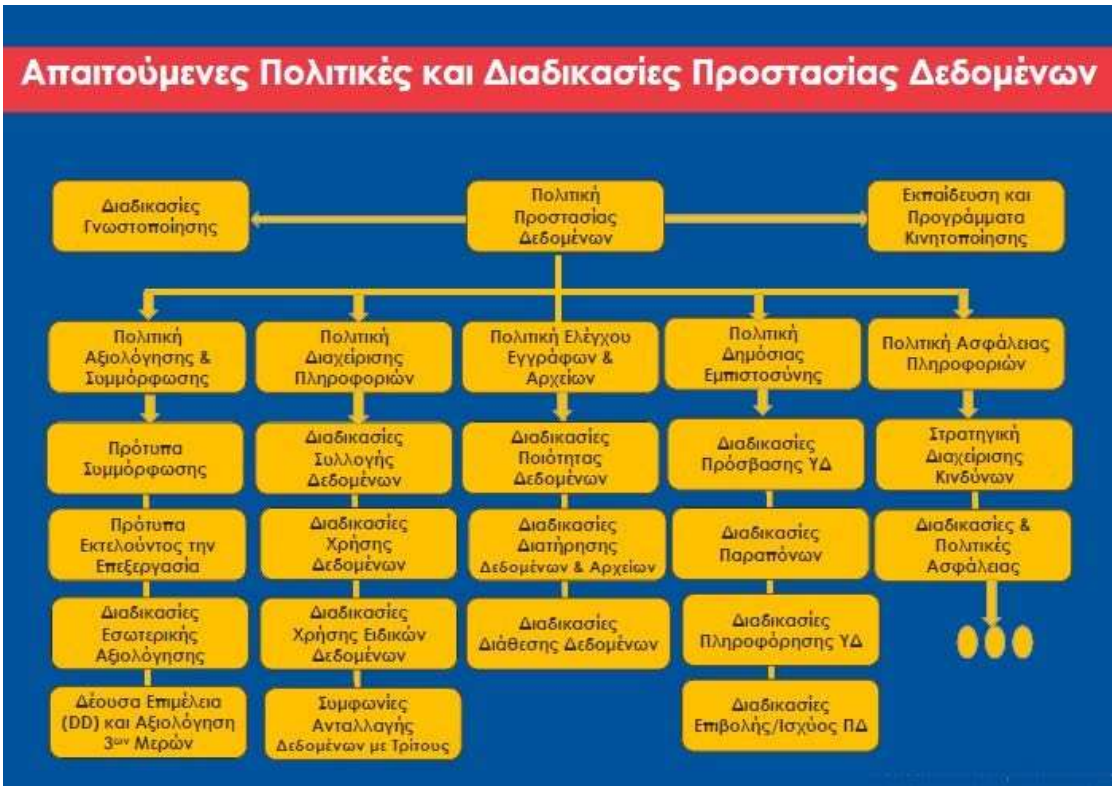
3) Την **αναβάθμιση των υποδομών ασφαλείας της**,

4) Την **αναθεώρηση σύνταξης των πολιτικών και των διαδικασιών της** και

5) Την **προσαρμογή της συνεχούς εκπαίδευσης του προσωπικού της**.

➢ Απαιτούμενες Πολιτικές και Διαδικασίες Προστασίας Προσωπικών δεδομένων

Οι διαδικασίες που πρέπει να επαναπροσδιορίσουν ή αν δεν υπάρχουν να δημιουργηθούν εξαρχής για να υλοποιήσουν το στόχο, φαίνονται στην εικόνα που ακολουθεί:



Εικόνα 18: Απαιτούμενες Πολιτικές και Διαδικασίες

Οι βασικοί άξονες του οποίους επιδιώκει να συμπεριλάβει και να εντάξει στη στρατηγική της η εν λόγω οντότητα είναι επιγραμματικά:

1) Η διαμόρφωση μιας πολιτικής αξιολόγησής της και συμμόρφωσής της με τον Κανονισμό, με την θέσπιση προτύπων συμμόρφωσης και διαδικασιών εσωτερικής αξιολόγησης.

2) Ο σχεδιασμός μιας πολιτικής για ορθολογικότερη και αποτελεσματικότερη διαχείριση των πληροφοριών, που περιλαμβάνουν τη συλλογή, χρήση και ανταλλαγή προσωπικών δεδομένων.

3) Η αναβάθμιση της πολιτικής ελέγχου των εγγράφων και των αρχείων προσωπικών δεδομένων της εταιρείας, εξασφαλίζοντας την ποιότητα, τη διατήρηση και τη διάθεση των δεδομένων.

4) Η δημιουργία μια πολιτικής δημόσιας εμπιστοσύνης, ώστε να διασφαλίζεται η πρόσβαση των υπευθύνων των δεδομένων, η έγκαιρη ενημέρωση και πληροφόρηση αυτών και η δυνατότητα διατύπωσης παραπόνων προς αυτούς.

5) Ο εκσυγχρονισμός της πολιτικής ασφαλείας των πληροφοριών μέσω στρατηγικών διαχείρισης κινδύνων, καθώς και αναβάθμιση των διαδικασιών και των πολιτικών ελέγχου ασφαλείας.

- Συγγραφή Μελέτης Αντικτύπου Ιδιωτικότητας (DPIA)

Εφαρμόζοντας το άρθρο 35 του GDPR, η φαρμακευτική εταιρεία συντάσσει την μελέτη επίπτωσης προστασίας των προσωπικών δεδομένων, αξιολογώντας τους κινδύνους ανά κατηγορία προσωπικών δεδομένων ή ανά έργο-προϊόν και αναγνωρίζοντας τους κινδύνους ποσοτικά ή εκτιμώντας τις επιπτώσεις τους σχετικά με την προστασία δεδομένων.

Η συγκεκριμένη μελέτη είναι απαραίτητη σε περιπτώσεις που εμπλέκονται ευαίσθητα προσωπικά δεδομένα, όπου γίνεται κατηγοριοποίηση με βάση το προφίλ των υποκειμένων (profiling) ή εμπλέκονται κίνδυνοι νομικών επιπτώσεων από τη χρήση νέων τεχνολογιών. Επιπλέον, αποτελεί μια ολοκληρωμένη αναφορά για τη Διοίκηση, τα ανώτατα στελέχη της εταιρείας και τον DPO, αφού επιτυγχάνεται ο προσδιορισμός των απαραίτητων ενεργειών και των οργανωτικών και τεχνικών μέτρων αποκατάστασης που θα πρέπει να εκτελεστούν. Ωστόσο, η DPIA θα πρέπει να επαναλαμβάνεται τακτικά ώστε να επικαιροποιείται και να συσχετίζεται και με άλλες εκτιμήσεις κινδύνων.

- Μηχανισμοί Διαβίβασης Δεδομένων σε Τρίτες Χώρες

Κατά τη σύνταξη της DPIA, θα πρέπει να συνυπολογίζονται και οι μηχανισμοί μεταφοράς δεδομένων σε τρίτες χώρες εκτός της ΕΕ.

Για τη διασφάλιση της μεταφοράς των δεδομένων σε τρίτους, η εταιρεία θέσπισε αυστηρότερες προϋποθέσεις και μηχανισμούς, όπως την ύπαρξη εταιρικών δεσμευτικών κανόνων (BCRs), πιστοποιήσεων και κωδικών ασφαλείας (π.χ. Privacy

Shield), πρότυπων συμβατικών ρητρών (SCCs), ισοδύναμων αποφάσεων –

εγγυήσεων και τις σχετικές αποφάσεις τρίτων χωρών.

Εικόνα 19: Χρονοδιάγραμμα Εξέλιξης 2ης Φάσης GDPR στην ελληνική φαρμακευτική εταιρεία [23/11/2017]

3) Τρίτη φάση: Υλοποίηση του GDPR

Στην τρίτη και τελευταία φάση, η οντότητα έδωσε έμφαση στην υλοποίηση θεμάτων πληροφορικής, εισάγοντας τη χρήση «ψευδωνυμοποίησης», δηλαδή επεξεργασία των δεδομένων προσωπικού χαρακτήρα με τρόπο ώστε τα δεδομένα να μην μπορούν να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες, διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο φυσικό πρόσωπο, π.χ χρήση αρχικών Α.Ε. Ακόμη, η εταιρεία εισήγαγε την έννοια της «ανωνυμοποίησης» και «κρυπτογράφησης» των δεδομένων ώστε να διασφαλιστεί η προστασία αυτών είτε πρόκειται για ευαίσθητα ή μη δεδομένα

- IT Λύσεις Ιδιωτικότητας πληροφοριακών Συστημάτων

Για την αναβάθμιση και τον εκσυγχρονισμό των συστημάτων της, η εταιρεία έχει ενσωματώσει πληροφοριακά συστήματα και εφαρμογές για την κρυπτογράφηση και απόκρυψη των δεδομένων και των e-mail της, τον έλεγχο μεταφοράς των δεδομένων, τη χαρτογράφηση της ροής των δεδομένων και τη μελέτη των επιπτώσεων αυτών. Επίσης, έχει εξασφαλίσει την ασφαλή αναζήτηση, αποθήκευση και ταξινόμηση των δεδομένων, τη διαγραφή και φορητότητα αυτών, καθώς και την εξασφάλιση των δικαιωμάτων των πελατών της ως προς τα προσωπικά τους δεδομένα.

- Συνεχής Επιθεώρηση και Παρακολούθηση του Προγράμματος (Auditing and Monitoring)

Σε όλη τη διάρκεια του σχεδιασμού της στρατηγικής, της αξιολόγησης και της υλοποίησης της, υπάρχει μια συνεχής ανάδραση και παρακολούθηση των βημάτων και της προετοιμασίας συμμόρφωσης με τον GDPR, ώστε να μπορούν να βελτιώνονται, να αλλάζουν ή να τροποποιούνται διαδικασίες που κρίνονται απαραίτητες για την εκπλήρωση του τελικού στόχου.

- Ο Οδικός Χάρτης (Roadmap) για την Υλοποίηση του GDPR

Τα 25 Βήματα για την Υλοποίηση του GDPR φαίνονται στην παρακάτω εικόνα, που αποτελεί και τον βασικό οδηγό διαμόρφωσης, σχεδιασμού και υλοποίησης στρατηγικής για την εν λόγω οικονομική οντότητα.

Εικόνα 20: Τα 25 βήματα του Οδικού Χάρτη Υλοποίησης του GDPR στην ελληνική φαρμακευτική εταιρεία

Επιγραμματικά, επιδιώκεται αρχικά η οικοδόμηση του έργου και της ομάδας που θα συμμετέχει σε αυτό με κατανομή των πόρων, προϋπολογισμό του χρόνου και του κόστους που θα απορροφήσει το έργο και κατανομή των ρόλων στους εργαζομένους, στους υπευθύνους και στον DPO.

Στη συνέχεια, γίνεται μια πρώτη εκτίμηση των κινδύνων μέσω της χαρτογράφησης και της απογραφής των δεδομένων και αναπτύσσονται πολιτικές και διαδικασίες ώστε να κινητοποιηθούν οι εργαζόμενοι στην αποτελεσματικότερη εφαρμογή τους.

Ακόμα, σχεδιάζονται και υλοποιούνται οι απαραίτητοι λειτουργικοί έλεγχοι για τη διασφάλιση των δικαιωμάτων των υποκειμένων και των προσωπικών τους στοιχείων και πραγματοποιούνται οι απαραίτητες ενέργειες για τη διαχείριση και την ενίσχυση των ελέγχων αυτών.

Τέλος, μέσω προσομοιώσεων και εκπαιδευτικών προγραμμάτων, ενισχύεται η διαρκής συμμόρφωση και η αξιολόγηση των ανθρώπινων πόρων της εταιρείας ως προς την αποτελεσματικότητα και την ετοιμότητά τους για την ενσωμάτωση του GDPR.

- <u>GDPR Stress Testing</u>

Πραγματοποιήθηκε από την εταιρία, σύμφωνα με τον σχεδιασμό της, στην τελευταία φάση του έργου τον Απρίλιο του 2018 λίγο πριν δηλαδή την καθολική ισχύ του Κανονισμού, και αφορά κάποια σενάρια «προσομοίωσης» για τον έλεγχο της ετοιμότητας της εταιρίας σε κάθε ένα από τα βασικά σημεία που απαιτούν προσοχή.

Περιλαμβάνει 3 διαφορετικές περιπτώσεις:

1) <u>Επίσκεψη της Αρχής Προστασίας Δεδομένων (Data protection authority visit)</u>

❖ Αντικείμενο: Προσομοίωση επίσκεψης της Αρχής για τον καθορισμό της ελαστικότητας στην εφαρμογή των μέτρων και των κανόνων συμμόρφωσης με τον Κανονισμό.

❖ Βήματα: Αρχικά πραγματοποιείται η έρευνα όπως ορίζεται από την προσομοίωση, καταγράφονται τα πρώτα ευρήματα και κατατίθενται οι απόψεις και οι παρατηρήσεις των εμπλεκομένων στην προσομοίωση γύρω από αυτά. Έπειτα, μέσω των συζητήσεων καταγράφονται τα καθοριστικά ευρήματα της έρευνας και πραγματοποιείται ανάλυση του αντικτύπου από τη δημοσίευση αυτών, καθώς και των επιπτώσεων από την εφαρμογή του νέου Κανονισμού.

❖ Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας, την ανάλυση του δημόσιου αντικτύπου και την ανάλυση των μέτρων εφαρμογής.

2) <u>Προσομοίωση παραβίασης δεδομένων (Data breach simulation)</u>

❖ Αντικείμενο: Προσομοίωση και παρακολούθηση παραβίασης προσωπικών δεδομένων με σκοπό τον προσδιορισμό της κατάστασης της τρέχουσας διαδικασίας.

❖ Βήματα: Αρχικά προσομοιώνεται η κατάσταση παραβίασης των προσωπικών δεδομένων και ενεργοποιούνται οι μηχανισμοί ειδοποίησης στο εσωτερικό της εταιρείας. Στη συνέχεια εξετάζεται η αποτελεσματικότητα της συνεχούς παρακολούθησης τέτοιων περιστατικών από την εταιρεία, αναλύονται τα ευρήματα της ετοιμότητας και των χειρισμών του προσωπικού και υποβάλλεται η τελική έκθεση.

❖ Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας και ταυτόχρονα πραγματοποιείται εκπαίδευση των υπαλλήλων για το χειρισμό παραβιάσεων προσωπικών δεδομένων.

3) <u>Δημόσια δράση (Public action)</u>

❖ Αντικείμενο: Προσομοίωση επίσκεψης της Αρχής για τον καθορισμό της ελαστικότητας στην εφαρμογή των μέτρων και των κανόνων συμμόρφωσης με τον Κανονισμό.

❖ Βήματα: Σε πρώτο στάδιο προσομοιώνεται ο τρόπος άσκησης των δικαιωμάτων των υποκειμένων και ελέγχεται η πρόσβαση στα προσωπικά τους δεδομένα, η δυνατότητα διόρθωσης, διαγραφής και ο αποκλεισμός από αυτά. Έπειτα, πραγματοποιείται η προσομοίωση δημόσιων συμβάντων με σκοπό τον έλεγχο ετοιμότητας και επίγνωσης των διαδικασιών που ακολουθούνται από τους εργαζομένους και τους υπευθύνους της εταιρείας.

❖ Αποτέλεσμα: Μία έκθεση που περιέχει τα ευρήματα της έρευνας, την ανάλυση του δημόσιου αντικτύπου και την ανάλυση των μέτρων εφαρμογής.

➢ <u>Διαμόρφωση Κώδικα Επιχειρηματικής Συμπεριφοράς για προσωπικά δεδομένα</u>

Τελευταίο και σημαντικότερο στη φάση υλοποίησης της στρατηγικής της εταιρείας για την συμμόρφωση με τον GDPR, είναι η δημιουργία και η διαμόρφωση ενός εταιρικού κώδικα δεοντολογίας, πέρα από τις πιστοποιήσεις και τα ISO που αποκτά. Η συγκεκριμένη εταιρεία ακολουθεί και προσαρμόζει κατά βάση στην κουλτούρα και την οργάνωσή της εταιρικούς και κλαδικούς κώδικες δεοντολογίας και επιχειρηματικής συμπεριφοράς, όπως για παράδειγμα των Κώδικα EFPIA για τα προσωπικά δεδομένα, που αποτελεί παράρτημα του Κώδικα των Συνδέσμων Φαρμακευτικών Εταιρειών Ελλάδας (ΣΦΕΕ).,

Ο Κώδικας Δεοντολογίας του ΣΦΕΕ, περιλαμβάνει τις ουσιαστικές ρυθμίσεις για την προώθηση των συνταγογραφούμενων φαρμάκων, τη δημοσιοποίηση των παροχών από φαρμακευτικές επιχειρήσεις προς Επαγγελματίες Υγείας και Επιστημονικούς Υγειονομικούς Φορείς, τη Διαδικασία Ελέγχου Εφαρμογής, τον ενδεικτικό υπολογισμό της αμοιβής των επαγγελματιών υγείας για παρεχόμενες υπηρεσίες σε φαρμακευτικές επιχειρήσεις και το μητρώο κλινικών μη παρεκβατικών μελετών.

➢ <u>Χρονοδιάγραμμα Υλοποίησης Έργου του GDPR</u>

Με την εφαρμογή όλων των παραπάνω μέτρων και διαδικασιών, η εν λόγω οντότητα επιδιώκει την ασφαλέστερη και ομαλότερη μετάβαση της στα νέα δεδομένα.

Στην εικόνα, παρουσιάζεται το τελικό χρονοδιάγραμμα υλοποίησης του έργου της με τα βήματα που ακολουθήθηκαν και που περιγράφηκαν αναλυτικότερα

προηγουμένως, από την έναρξη των διαδικασιών προσαρμογής της τον Απρίλιο του 2017 μέχρι και τον Μάιο του 2018 που θα έπρεπε να είναι έτοιμη να συμμορφωθεί πλήρως με το νέο Κανονισμό.

Εικόνα 21: Χρονοδιάγραμμα Υλοποίησης GDPR στην ελληνική φαρμακευτική εταιρεία [4/2017 – 5/2018]

Συνοψίζοντας, αξίζει να αναφέρουμε πως η εταιρεία και ο DPO, έδωσε ιδιαίτερη έμφαση στην εκπαίδευση όλου του προσωπικού που διαχειρίζεται προσωπικά δεδομένα, ώστε να ξέρει ανά πάσα στιγμή τι να πράξει. Η εκπαίδευση ξεκίνησε πυραμιδωτά, από πάνω προς τα κάτω, εντάσσοντας όλο σχεδόν το προσωπικό, στην ευαισθησία που λέγεται GDPR, αλλά φυσικά χρειάζεται ακόμη πολύ προσπάθεια για την πλήρη ένταξη του Κανονισμού στις λειτουργίες της εταιρίας.

Όσον αφορά, την αγορά εφαρμογών και προγράμματα υπολογιστών που θα δημιουργήσουν τεχνικές ανωνυμοποίησης, ψευδωνυμοποίησης, κρυπτογράφησης κ.α., είναι τοποθετημένο για τον τελευταίο μήνα, όπου θα παρουσιαστούν προτάσεις με εφαρμογές που είναι πιο κοντά στις απαιτήσεις τόσο του GDPR, όσο και της ίδιας της εταιρείας.

Σε ερώτηση μας σχετικά με τον αν χρειάζεται η υλοποίηση ασφαλιστικού συμβολαίου, ώστε να είναι προστατευμένη η εταιρία, ο κ. Ευαγγελίδης, απάντησε πως έχει δει τις μεγαλύτερες εταιρίες κάλυψης ασφαλιστικού κινδύνου διεθνώς που είναι εξειδικευμένες στο GDPR. Η ιδέα της κάλυψης του ασφαλιστικού κινδύνου, είναι μια ακριβής λύση η οποία δεν διασφαλίζει στο έπακρο την ασφάλεια της εταιρίας, διότι υπάρχουν πολλές καταστάσεις και «ψηλά γράμματα», που έχουν να κάνουν με ψηφιακές λύσεις που δεν οδηγούν πάντοτε προς την σωστή προσέγγιση. Συνεπώς η εκτίμησή του σε σχέση με το βεληνεκές της εταιρίας, είναι ότι δεν της χρειάζεται διότι είναι αρκετά δαπανηρή η ασφάλεια και η ετήσια συνδρομή, χωρίς να έχει πλήρη και ασφαλή αποτελέσματα.

Τέλος, ο κ. Ευαγγελίδης καταλήγει στο συμπέρασμα πως η εμφάνιση του GDPR έχει θετικό αντίκρισμα προς τις εταιρείες. Μπορεί να απαιτείται περισσότερη γραφειοκρατία, αλλά αυτό σημαίνει και περισσότερη ασφάλεια και προστασία των δεδομένων, από την πλευρά των πελατών, δημιουργώντας καλύτερο όνομα στην αγορά εργασίας. Φυσικά όλο πλαίσιο που ορίζει ο GDPR δεν μπορεί να υλοποιηθεί μόνο από ένα άτομα τον DPO. Αντίθετα πολύ σημαντικό είναι να χτιστεί μια ομάδα, να υπάρχουν κάποια άτομα που θα συνεργάζονται αρμονικά μεταξύ τους και με τον DPO, τα οποία θα είναι άξια εμπιστοσύνης και θα ενσωματωθούν μέσα στις δράσεις της κανονιστικής συμμόρφωσης και προστασίας γενικότερα των δεδομένων.

7.3 Εφαρμογή του GDPR από Ελληνική Τράπεζα

Οι Τράπεζες είναι ανάμεσα στις οντότητες που επηρεάζονται στο μέγιστο βαθμό από την εφαρμογή του GDPR καθώς έχουν στην κατοχή τους μεγάλο όγκο προσωπικών δεδομένων. Εκτός από τα υψηλά χρηματικά πρόστιμα, ένα κενό στην προστασία δεδομένων μιας τράπεζας, αν αποκαλυφθεί, μπορεί να οδηγήσει σε καταστροφικές συνέπειες στη φήμη της και στις σχέσεις της με την πελατεία της. Ειδικά στον Τραπεζικό Τομέα η φήμη είναι για κάποιες τράπεζες το σπουδαιότερο περιουσιακό αγαθό – έναντι των fintech εταιρειών.

Τα δεδομένα των πελατών μπορεί να κρατούνται σε περισσότερα από 100 διαφορετικά συστήματα. Με δεδομένο το γεγονός ότι οι αλλαγές σε κάθε ένα από αυτά τα συστήματα διαρκούν έως και αρκετούς μήνες για να υλοποιηθούν, γίνεται

αντιληπτός ο όγκος των εργασιών που πρέπει να ολοκληρωθούν σε σύντομο χρονικό διάστημα αλλά και η πολυπλοκότητα του.

Η υπό έρευνα τράπεζα, το όνομα της οποίας μας ζητήθηκε να μην αναφερθεί, αλλά στο εξής θα συναντάται ως «Τράπεζα», εφαρμόζει ήδη τα προβλεπόμενα στο ισχύον κανονιστικό και νομικό πλαίσιο, όπως απορρέουν από το Ν. 2472/1997, και τις αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ ή «Αρχή»).

Βασικός στόχος για τη συμμόρφωση με τον GDPR είναι ο εντοπισμός αποκλίσεων και η καταγραφή συγκεκριμένων ενεργειών ανά επιχειρησιακή περιοχή της Τράπεζας, με σκοπό την ευθυγράμμιση με τις απαιτήσεις του GDPR κατά την ημέρα της εφαρμογής του (25 Μαΐου 2018).

Για τη συμμόρφωση με τον Κανονισμό ενεπλάκησαν πολλές Μονάδες της Τράπεζας με στελέχη, μεταξύ άλλων, από τις παρακάτω Γενικές Διευθύνσεις:

- Γ. Διεύθυνση Κανονιστικής Συμμόρφωσης και Εταιρικής Διακυβέρνησης
- Γ. Διεύθυνση Νομικών Υπηρεσιών
- Γ. Διεύθυνση Ανθρώπινου Δυναμικού
- Γ. Διεύθυνση Λιανικής Τραπεζικής
- Γ. Διεύθυνση Λειτουργικής Στήριξης (υπάγονται οι Δ/νσεις Πληροφορικής και το Γραφείο CISO)

Επιπλέον η Τράπεζα προέβη και σε εκπαίδευση όλου του ανθρώπινου δυναμικού της, μέσω της εξ αποστάσεως εκπαίδευσης, ενώ στα σχέδια της Τράπεζας, είναι και η διενέργεια κάποιων σεμιναρίων για να διαπιστωθεί αν έχει κατανοηθεί ο Κανονισμός και κατά πόσο έχει επιτευχθεί σωστή συμμόρφωση, και δεν ελλοχεύει ο κίνδυνος της επιβολής προστίμων. Τέλος η ενημέρωση των πελατών της, έγινε με την αποστολή στον καθένα ξεχωριστά ενός μηνύματος ηλεκτρονικού αρχείου, που περιλάμβανε έντυπο ενημέρωσης πελάτη σχετικά με το τι είναι το GDPR και γιατί η Τράπεζα έχει ανάγκη από την συλλογή των προσωπικών δεδομένων για την συνέχιση της διενέργειας συναλλαγών και εξυπηρέτησης των πελατών τους.

7.3.1 Φάσεις που ακολουθήθηκαν για την συμμόρφωση με τον GDPR

Φάση 1: Χαρτογράφηση λειτουργιών επεξεργασίας προσωπικών δεδομένων

Στην πρώτη φάση, πραγματοποιήθηκε ένα είδος εσωτερικού ελέγχου, όπου ερευνήθηκαν οι επιχειρησιακές, τεχνικές και λειτουργικές διαδικασίες της Τράπεζας. Πραγματοποιήθηκαν συνεντεύξεις όλων των εμπλεκόμενων μερών, ώστε να αναγνωριστούν τα τμήματα όπου πραγματοποιείται επεξεργασία προσωπικών δεδομένων. Έγινε επισκόπηση όλων των διαθέσιμων επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών προκειμένου να γίνει κατανοητή η υφιστάμενη επεξεργασία προσωπικών δεδομένων και η σχετική τεχνολογική υποδομή, ώστε οι ιθύνοντες της Τράπεζας, να αναγνωρίσουν τους σχετικούς κινδύνους και τις δικλίδες ασφαλείας που απαιτούνται.

Εξετάστηκαν λεπτομερώς επίσης, το οργανόγραμμα και η εσωτερική δομή της Τράπεζας, καθώς και συνεργασίες που έχουν γίνει με εξωτερικούς συνεργάτες. Λήφθησαν πληροφορίες, για τους ρόλους και τις υποχρεώσεις της Τράπεζας καθώς και τις πολιτικές που ακολουθούνται σχετικά με τα προσωπικά δεδομένα. Πρωταρχικής σημασίας είναι, από πού συλλέγονται τα δεδομένα (πελάτες ή τρίτα άτομα κ.α.), αν πρόκειται για ευαίσθητα δεδομένα, και αν είναι απαραίτητη η συλλογή τους για την διατήρηση των συναλλακτικών σχέσεων με τους πελάτες τους.

Ένα από τα βασικά αποτελέσματα αυτού του σταδίου ήταν η δημιουργία και εμπλουτισμός του αρχείου δραστηριοτήτων προσωπικών δεδομένων (σε γενικό επίπεδο) της Τράπεζας, και η δημιουργία και ο εμπλουτισμός των καταλόγων δραστηριοτήτων και πόρων επεξεργασίας για τις επεξεργασίες προσωπικών δεδομένων υψηλού κινδύνου της. Ενδεικτικά αυτό το αρχείο περιλαμβάνει πληροφορίες σχετικά με:

- Το όνομα και τα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας, του εκπροσώπου του Υπεύθυνου Επεξεργασίας και του Υπεύθυνου Προστασίας Δεδομένων.
- Τους σκοπούς επεξεργασίας δεδομένων.
- Τις κατηγορίες των αποδεκτών στους οποίους έχουν ή πρόκειται να κοινοποιηθούν, συμπεριλαμβανομένων και αποδεκτών τρίτων χωρών ή διεθνών οργανισμών.

❖ Τα προβλεπόμενα χρονικά όρια για τη διαγραφή των διαφόρων κατηγοριών δεδομένων., αλλά και τις γενικές περιγραφές των τεχνικών και οργανωτικών δικλείδων ασφάλειας.

❖ Το όνομα και τα στοιχεία των Εκτελούντων ή των Υπεύθυνων Επεξεργασίας εκ μέρους των οποίων οι Εκτελούντες ενεργούν και, όπου υφίστανται, τα στοιχεία των εκπροσώπων των Εκτελούντων και των Υπεύθυνων Επεξεργασίας και του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων.

❖ Τις κατηγορίες επεξεργασίας δεδομένων που εκτελούνται εκ μέρους του κάθε Υπεύθυνου Επεξεργασίας.

Το όφελος σε αυτή τη φάση είναι ότι σχηματίσθηκε μια καθαρή εικόνα των ροών προσωπικών δεδομένων και στη συνέχεια έγινε η χαρτογράφηση αυτών. Τα διαγράμματα ροής προσωπικών δεδομένων αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, καταχώρηση, οργάνωση, χρήση, αποθήκευση, μεταφορά έως την καταστροφή τους.

Φάση 2: Μελέτη αποκλίσεων σε σχέση με τις απαιτήσεις του GDPR

Δια μέσου αυτής της φάσης, πραγματοποιήθηκε έγκαιρη αναγνώριση των βασικών κενών και περιοχών, που χρειάζονται βελτίωση στην Τράπεζα, ως προς την ορθή συμμόρφωση με τον Κανονισμό. Κάθε απόκλιση που αναγνωρίσθηκε ανά περιοχή ελέγχου, συνοδευόταν από μια σύντομη περιγραφή προκειμένου να αναγνωρισθούν γρήγορα τα πιθανά θέματα που σχετίζονται με τις αποκλίσεις αυτές.

Ειδικότερα πραγματοποιηθήκε διαγνωστική μελέτη των υφιστάμενων διαδικασιών, δεδομένων (και της διαβάθμισης τους) και συστημάτων πληροφορικής., αναγνώριση των σχετικών απαιτήσεων του GDPR ως προς τις περιοχές επεξεργασίας προσωπικών δεδομένων, καθώς και ανάλυση των αποκλίσεων σχετικά με την Προστασία Προσωπικών Δεδομένων σύμφωνα με τον Κανονισμό.

Φάση 3: Εκτίμηση αντικτύπου από την επιβολή του GDPR (DPIA)

Σε αυτή τη φάση, πραγματοποιήθηκε μελέτη των επιπτώσεων του GDPR, όπως ορίζει ο νέος Κανονισμός. Πραγματοποιήθηκε:

Ι. Περιγραφή των ροών πληροφορίας προσωπικών δεδομένων, δηλαδή καθορισμός του είδους της πληροφορίας που χρησιμοποιείται, του σκοπού για τον οποίο χρησιμοποιείται, του λήπτη της πληροφορίας και της οντότητας που

χρησιμοποιείται η πληροφορία. Ενδεικτικά κάποιες από τις έννοιες που εξετάστηκαν ήταν οι έννοιες της συγκατάθεσης και της επεξεργασίας των προσωπικών δεδομένων,

II. Αναγνώριση των σχετικών κινδύνων και αξιολόγηση τους σε επίπεδο φυσικών προσώπων (π.χ. ζημιά που ενδέχεται να προκληθεί από ανακριβή δεδομένα ή από παραβίαση ασφάλειας ή πρόκληση δυσαρέσκειας) και κίνδυνοι σε επίπεδο οργανισμού (απόκλιση συμμόρφωσης με κανονιστικές και νομικές ρυθμίσεις ή ζημιά στη φήμη του οργανισμού ή παραβίαση της ασφάλειας προσωπικών δεδομένων με τελικό αποτέλεσμα την πρόκληση σημαντικού οικονομικού κόστους).

III. Αναγνώριση και αξιολόγηση λύσεων σχετικά με την προστασία προσωπικών δεδομένων και αξιολόγηση του τρόπου που κάθε κίνδυνος μπορεί να αντιμετωπιστεί ή να μετριασθεί σε αποδεκτά επίπεδα.

Με βάση τα αποτελέσματα των προηγούμενων φάσεων διενεργείται εκτίμηση των επιπτώσεων κατά περίπτωση (δηλαδή για τις περιοχές επεξεργασίας δεδομένων υψηλού κινδύνου). Για κάθε εύρημα, συντάσσονται οι αντίστοιχες διορθωτικές ενέργειες.

Φάση 4: Καθορισμός σχεδίου επίλυσης των αποκλίσεων

Σύμφωνα με τα αποτελέσματα που προήλθαν από την προηγούμενη φάση, καταγράφηκε αναλυτικό και σαφές σχέδιο στο οποίο περιλαμβάνονται οι προτάσεις βελτίωσης ανά περιοχή / κατάστημα της Τράπεζας, με σκοπό την αντιμετώπιση των ελλείψεων ή και των αποκλίσεων σε σχέση με τις απαιτήσεις του GDPR.Το σχέδιο επέτρεψε στην Τράπεζα να ορίσει προτεραιότητες σχετικά με τις διορθωτικές ενέργειες για την αποτελεσματική και αποδοτική κάλυψη των αποκλίσεων.

Έτσι η Τράπεζα καθόρισε μια μακροπρόθεσμη στρατηγικλη συμμόρφωσης με τον GDPR, Δημιουργήθηκε ένα αναλυτικό και σαφές σχέδιο, με την δημιουργία μίας λίστας με αποκλίσεις που πρέπει να διορθωθούν, καθώς και μιας λίστας με τον προσδιορισμό συγκεκριμένων εργασιών που πρέπει να γίνουν, ώστε να βελτιωθεί κατά τον δυνατόν και πιο άμεσα τα επίπεδο συμμόρφωσης με τον GDPR. Μέσω της χρήσης διαγνωστικών εργαλείων και μέσων επικεντρωμένα στη συμμόρφωση με τον Κανονισμό επιτεύχθηκε η ανεύρεση των δεδομένων που χρησιμοποιούνται στο περιβάλλον της Τράπεζας καθώς και στην αποτύπωση των ροών της.

Φάση 5: Υλοποίηση σχεδίου επίλυσης των αποκλίσεων

Σε αυτή τη φάση, γίνεται εφαρμογή του σχεδίου που καταρτίστηκε στην προηγούμενη φάση. Συγκεκριμένα πραγματοποιήθηκαν οι εξής ενέργειες:

- Βελτίωση Πολιτικής Ασφαλείας Δεδομένων η οποία στοχεύει στην διασφάλιση της ασφαλής τήρησης, επεξεργασίας και μετάδοσης των πληροφοριών, καθώς και στην εξασφαλίση της πλήρης συμμόρφωσης της Τράπεζας με τις σχετικές κείμενες νομικές και κανονιστικές απαιτήσεις. Έτσι επυτγχάνεται προστασία της Τράπεζας και όσων συναλλάσσονται με αυτή για την χρήση και διακίνηση των προσωπικών δεδομένων τους και στον άμεσο και αποτελεσματικό χειρισμό περιστατικών παραβιάσεων ασφαλείας.
- Κώδικας Δεοντολογίας σχετικά με την Επεξεργασία Προσωπικών Δεδομένων
- Τροποποίηση Συμβάσεων και Συμβολαίων

Η Τράπεζα επέλεξε να χρησιμοποιήσει τις ήδη υφιστάμενες μηχανογραφικές εφαρμογές που διαθέτει και όχι να προσφύγει στην αγορά κάποιας νέας εφαρμογής. Προτιμήθηκε σε συνεργασία με την εταιρία λογισμικού η αναβάθμιση της ήδη υπάρσχουσας εφαρμογής με την εναρμόνισή της στις διατάξεις του GDPR. Συγκεκριμένα, χρησιμοποιήθηκαν λύσεις για:

- Ανίχνευση προσωπικών δεδομένων.
- Κρυπτογράφηση και ψευδωνυμοποίηση.
- Προστασίας Διαρροής Δεδομένων.
- Ενίσχυσης της περιμετρικής ασφάλειας για αποτροπή και ανίχνευση παραβιάσεων που θα μπορούσαν να οδηγήσουν σε κλοπή, απώλεια ή αθέμιτη τροποποίηση προσωπικών δεδομένων.

Φάση 6: Εκπαίδευση

Στη φάση αυτή η Τράπεζα όφειλε να εκπαιδεύσει το ανθρώπινο δυναμικό της όσον αφορά στο τι είναι το GDPR και ποιες αλλαγές φέρει. Η μέθοδος που επιλέχθηκε, ήταν η εξ αποστάσεως τηλεεκπαίδευση, καθώς και η υλοποίηση εκπαιδευτικού σεμιναρίου, με την συμμετοχή εκπροσώπων όλων των εμπλεκόμενων Διευθύνσεων της Τράπεζας. Σκοπός δεν είναι μόνο η ενημέρωση-εκπαίδευση του ανθρώπινου δυναμικού της Τράπεζας, αλλά και η ευαισθητοποίηση του προσωπικού σχετικά με την διαχείριση των ευαίσθητων δεδομένων.

Στο εκπαιδευτικό σεμινάριο, πραγματοποιήθηκαν οι εξής ενέργειες:

✓ Εφαρμογή των βασικών άρθρων του κανονισμού στο περιβάλλον της Τράπεζας.

✓ Εκπαίδευση σε σχέση με τα εργαλεία που υποστηρίζουν τη συμμόρφωση με τις απαιτήσεις του GDPR.

✓ Εκπαίδευση για την υλοποίηση πλαισίου παρακολούθησης των απαιτήσεων συμμόρφωσης με τον GDPR.

✓ Παροχή του κατάλληλου εκπαιδευτικού υλικού υπό διαδικτυακή μορφή.

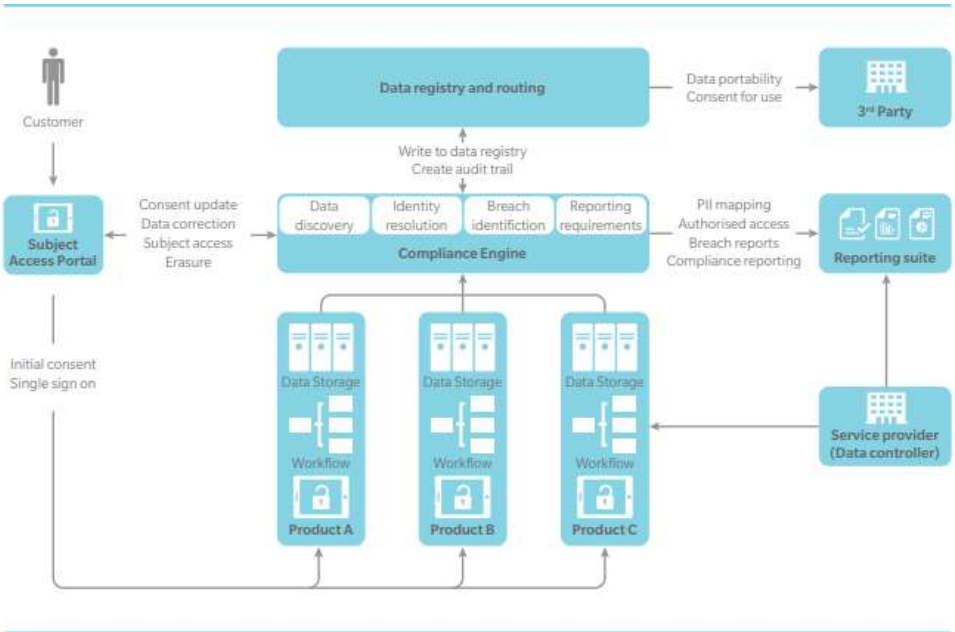
Φάση 7: Δειγματοληπτικός έλεγχος και καταγραφή διορθωτικών ενεργειών

Στη φάση αυτή εκπονήθηκε ένα ολοκληρωμένο πρόγραμμα για τη διενέργεια ελέγχων συμμορφώσεως των Μονάδων της Τράπεζας βάσει των απαιτήσεων του Κανονισμού. Συγκεκριμένα, πραγματοποιήθηκε:

1) Ανάπτυξη προγράμματος διενέργειας ελέγχων συμμορφώσεως των Μονάδων της τράπεζας, σύμφωνα με τις απαιτήσεις του Κανονισμού.

2) Υλοποίηση δειγματοληπτικού ελέγχου διαδικασιών και συστημάτων για εντοπισμό τυχόν ελλείψεων.

3) Περιγραφή διορθωτικών ενεργειών για αποκατάσταση τυχόν ευρημάτων από τον δειγματοληπτικό έλεγχο.



Εικόνα: «Μια βιώσιμη λύση GDPR σε ένα διασυνδεδεμένο οικονομικό οικοσύστημα» Πηγή: (Wyman , Ivell , Wilkinson , & Helps , 2017)

7.3.2 GDPR και PSD II

Οι Τράπεζες, λόγω του ιδιόμορφου χαρακτήρα τους, με την διαχείριση χρημάτων, εκτός από τον νέο Κανονισμό, έχουν να αντιμετωπίσουν και το PSD II ((Payment Service Directive II). Εν συντομία η PSD II, που εφαρμόζεται από 13 Ιανουαρίου του 2018 σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης, επιτρέπει στους πελάτες των Τραπεζών, είτε απλούς καταναλωτές είτε επιχειρήσεις, να χρησιμοποιούν τρίτους παρόχους για παροχή οικονομικών υπηρεσιών. Θα μπορεί κάποιος χρησιμοποιώντας το Facebook ή το Google να πληρώνει τους λογαριασμούς του, να πραγματοποιεί P2P (Peer-to-Peer)[18] συναλλαγές και να έχει ανάλυση των εξόδων του και των υπολοίπων των λογαριασμών του, ενώ τα χρήματα του είναι με ασφάλεια στον τραπεζικό του λογαριασμό. Οι Τράπεζες (στην PSD II είναι υποχρεωμένες να παρέχουν σε αυτούς, τους τρίτους παρόχους πρόσβαση στους λογαριασμούς των πελατών τους μέσω API (Application Program Interface). Έτσι, αυτοί οι τρίτοι θα μπορούν να δημιουργήσουν οικονομικές υπηρεσίες πάνω στα δεδομένα και τις πληροφοριακές υποδομές των Τραπεζών ανάμεσα στις εμπλεκόμενες επιχειρήσεις και τις τράπεζες, οι τελευταίες θα έχουν πολύ περιορισμένο έλεγχο στο πως θα διαχειρίζονται οι τρίτοι τα δεδομένα. Οι Τράπεζες πλέον θα ανταγωνίζονται όχι μόνο άλλες Τράπεζες αλλά οποιονδήποτε προσφέρει οικονομικές υπηρεσίες. Το PSD II έχει αλλάξει ριζικά τον παραδοσιακό τρόπο που γινόντουσαν οι πληρωμές. Μέσω του PSD II η Ευρωπαϊκή Επιτροπή στοχεύει στο να προάγει την καινοτομία, να ενισχύσει την προστασία των συμφερόντων του καταναλωτή και να βελτιώσει την ασφάλεια των πληρωμών μέσω του διαδικτύου και την πρόσβαση σε λογαριασμούς εντός της Ευρωπαϊκής Ένωσης.

Κατά συνέπεια η PSD II και GDPR έρχονται να κάνουν ακόμη πιο επίπονη την προσπάθεια που καταβάλουν οι τράπεζες στο πλαίσιο του ψηφιακού μετασχηματισμού τους. Είναι δύο κανονιστικές υποχρεώσεις οι οποίες φαίνεται να σπρώχνουν τις τράπεζες προς αντίθετες κατευθύνσεις. Από τη μια η PSD II υποχρεώνει τις τράπεζες να «ανοίξουν» τα δεδομένα των πελατών τους συμπεριλαμβανομένων των λογαριασμών τους, που παραδοσιακά μόνο αυτές

[18] P2P (Peer-to-Peer) στην Οικονομία, είναι ένα αποκεντρωμένο μοντέλο συναλλαγών όπου οι συναλλασσόμενοι πραγματοποιούν συναλλαγές απευθείας ο ένας με τον άλλον

ήλεγχαν σε τρίτες εταιρείες, και από την άλλη ο GDPR θέτει αυστηρές απαιτήσεις συνοδευόμενες από βαριά πρόστιμα για την προστασία των δεδομένων των πελατών.

Ενώ οι «ψηφιακοί έμποροι» είναι ενθουσιασμένοι στην ευκαιρία που προσφέρεται από την PSD II να αυξήσουν τις πωλήσεις τους χρησιμοποιώντας τα δεδομένα και τα μεταδεδομένα των πελατών τους, ο GDPR το απαγορεύει αν δεν υπάρχει η σαφής συγκατάθεση του πελάτη, με οριοθετημένο σκοπό και διάρκεια. Ο πελάτης θα μπορεί επιπλέον να άρει την συγκατάθεση που είχε δώσει νωρίτερα και να απαιτήσει την διαγραφή όλων των προσωπικών του δεδομένων από την τράπεζα ή τον τρίτο πάροχο. Τόσο οι οργανισμοί (στην συγκεκριμένη περίπτωση οι τράπεζες) όσο και οι τρίτοι πάροχοι πρέπει να έχουν την σαφή και ρητή συγκατάθεση του πελάτη προκειμένου να χρησιμοποιήσουν τα δεδομένα του. Η συγκατάθεση αφορά και στον τρόπο που θα χρησιμοποιηθούν τα δεδομένα του πελάτη. Αν τα δεδομένα χρησιμοποιηθούν από τρίτο πάροχο πρέπει να υπάρχει η συγκατάθεση και για το ποιος είναι αυτός ο πάροχος και το πώς θα χρησιμοποιηθούν τα δεδομένα του από αυτόν.

Οι οργανισμοί και οι εταιρείες θα πρέπει να είναι σε θέση να διαχειριστούν το δικαίωμα που έχει κάθε άτομο να μπορεί να αναιρέσει τη συγκατάθεση του. Πρακτικά αυτό σημαίνει ότι οι επιχειρήσεις θα πρέπει να είναι σε θέση να σταματήσουν αμέσως την χρήση των δεδομένων του ατόμου και σε κάποιες περιπτώσεις να μπορούν να διαγράφουν τα δεδομένα από τον οργανισμό, με την χρήση για παράδειγμα, συστημάτων διαχείρισης συγκατάθεσης» (Consent Management System) τα οποία εστιάζουν στη διευκόλυνση των εταιρειών για αποτελεσματική διαχείριση της συγκατάθεσης.

Αποτέλεσμα όλων αυτών των ενεργειών, είναι να αυξάνεται ο κίνδυνος των Τραπεζών που πηγάζει από τον ρόλο τους ως θεματοφύλακα των δεδομένων των πελατών τους. Ακόμη και αν ο τρίτος πάροχος είναι η αιτία μη συμμόρφωσης με τις απαιτήσεις του GDPR και η τράπεζα μπορεί να αποδείξει ότι είχε πράξει όλα τα προβλεπόμενα από τον κανονισμό (πρακτικά οι οργανισμοί δύσκολα μπορούν να αντέξουν σε ένα τέτοιο έλεγχο), η βλάβη στη φήμη και οι συνέπειες της θα επηρεάσει περισσότερο την τράπεζα παρά τον τρίτο (που θα μπορούσε να είναι και μια νεοφυής εταιρεία fintech). Αυτό θα συμβεί γιατί η κοινή γνώμη έχει την αντίληψη ότι, είναι ευθύνη της τράπεζας η προστασία των δεδομένων των πελατών της. Ακόμη και αν

υπάρχει η ρητή συγκατάθεση του πελάτη, δεν θα είναι κατανοητές οι συνέπειες της ενέργειας του σε ένα τόσο πολύπλοκο οικοσύστημα «ανοιχτής τραπεζικής» και τελικά η ευθύνη θα γυρίσει στις τράπεζες. (Gartner, 2017)

Η ρητή συγκατάθεση, ο σκοπός και η διάρκεια πρέπει να μπορούν να αποδειχτούν προκειμένου η τράπεζα να μπορεί να αμυνθεί σε μια διένεξη με τον πελάτη ή σε περίπτωση κακής χρήσης του API της τράπεζας από τον τρίτο πάροχο. Παρόμοια και όπου το δικαίωμα στη λήθη δεν μπορεί να εφαρμοσθεί λόγω κανονιστικών απαιτήσεων, οι τράπεζες θα πρέπει να είναι σε θέση να αποδείξουν στον έλεγχο της Ρυθμιστικής Αρχής ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των δεδομένων.

7.4 Σύνοψη

Στο παρόν κεφάλαιο, επιδιώχθηκε να παρουσιαστεί η εφαρμογή της μεθοδολογίας συμμόρφωσης με τον GDPR όπως σχεδιάστηκε και υλοποιήθηκε τόσο από μια ελληνική φαρμακευτική εταιρεία, όσο και από μια εγχώρια συστημική Τράπεζα και να συσχετιστεί η θεωρία με την πράξη.

Διαπιστώθηκε ότι τα κύρια σημεία υλοποίησης της στρατηγικής συμμόρφωσης με τον Κανονισμό παραμένουν κατά πλειοψηφία ίδια και για την φαρμακευτική εταιρία και για την Τράπεζα τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, ενώ ο βασικός πυρήνας για την πραγματοποίηση του μέχρι το τελικό στάδιο, είναι η διαμόρφωση μιας ενιαίας αντίληψης και κουλτούρας του προσωπικού μέσα στην επιχείρηση.

Επιπρόσθετα παρουσιάστηκε και η επιπλέον δυσκολία που έχουν να αντιμετωπίσουν οι Τράπεζες, με την προσθήκη εκτός του GDPR και του PSD II. Και οι δύο μελέτες περιπτώσεων, έδειξαν ότι:

- ✓ Η επιτυχία της συμμόρφωσης με τον Κανονισμό εξαρτάται από την υποστήριξη της ανώτατης διοίκησης της Τράπεζας,
- ✓ Την ικανότητα και ωριμότητα που έχουν οι τράπεζες να ανταποκρίνονται γρήγορα και να προσαρμόζονται στις αλλαγές στο ρυθμιστικό περιβάλλον,
- ✓ Ότι ο υψηλός βαθμός ασφάλειας και οι καλά σχεδιασμένες διαδικασίες αποτελούν σημαντικό ανταγωνιστικό πλεονέκτημα,

- ✓ Ότι ο Κανονισμός περιέχει ασάφειες οι οποίες πρέπει να διευκρινιστούν,
- ✓ Η συμμόρφωση με τον κανονισμό είναι μια συνεχής διαδικασία η οποία δεν θα έχει ημερομηνία λήξης τουλάχιστον για όσο διάστημα είναι σε ισχύ ο Κανονισμός.

ΚΕΦΑΛΑΙΟ 8 : ΣΥΜΠΕΡΑΣΜΑΤΑ

8.1 Συμπεράσματα

Ανακεφαλαιώνοντας, η αλματώδης πρόοδος της τεχνολογίας με την εφεύρεση νέων μηχανών και εφαρμογών, αδιαμφισβήτητα κάνουν πιο εύκολη των καθημερινότητα των πολιτών και επιφέρουν μια σειρά από θετικές επιπτώσεις στο σύνολο της κοινωνίας αλλά και της οικονομικής πολιτικής. Ταυτόχρονα όμως, δημιουργούν «γκρίζες ζώνες» που περιλαμβάνουν την προστασία της ιδιωτικότητας και την ασφάλεια των προσωπικών δεδομένων τους. Προκειμένου να επιτευχθεί ισορροπία μεταξύ των ανωτέρω, η νομοθετική εξουσία διαδραματίζει καθοριστικό ρόλο.

Κατά τη διάρκεια της εκπόνησης της διπλωματικής εργασίας διαπιστώθηκε ότι τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο γύρω από τα προσωπικά δεδομένα υφίσταται ένα ισχυρό νομικό και θεσμικό "πλέγμα" προστασίας, το οποίο προσπαθεί να αντιμετωπίσει τις προκλήσεις που προκύπτουν από τις σύγχρονες τεχνολογικές απαιτήσεις. Στο πλαίσιο λοιπόν των σύγχρονων απαιτήσεων, θεσμοθετήθηκε ο Γενικός Κανονισμός 2016/679 ΕΕ, ο οποίος είναι κατ' ουσίαν ένα νομοθέτημα εκτενές, σαφές και αναλυτικό, απόρροια μεγάλης και επίπονης προσπάθειας προς την κατεύθυνση της συνεκτικής ρύθμισης του ζητήματος της προστασίας των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Απλοποιεί διαδικασίες, μειώνει τη γραφειοκρατία, ενισχύει το ρόλο των εποπτικών αρχών, δημιουργεί νέους θεσμούς και επαναπροσδιορίζει αρμοδιότητες και εξουσίες.

Δεν μπορεί, ωστόσο, να συμπεριλάβει τις ιδιαιτερότητες των κρατών μελών, που πρέπει να τροποποιήσουν, να συμπληρώσουν, να προσαρμόσουν την εθνική τους νομοθεσία σε μικρό ή μεγάλο βαθμό, να επαναδιατυπώσουν τον ρόλο των εποπτικών τους Αρχών, να ιδρύσουν εποπτικές Αρχές, ή και να προβούν σε οποιεσδήποτε άλλες ειδικές ρυθμίσεις. Είναι αναγκαία, συνεπώς, η δέουσα προετοιμασία εκ μέρους των κρατών μελών, στο νομοπαρασκευαστικό τομέα και η έγκαιρη διαμόρφωση των

συνθηκών εφαρμογής του Κανονισμού, όπως η ενίσχυση των εθνικών εποπτικών Αρχών και η ενημέρωση των φορέων, είτε πρόκειται για ιδιωτικούς, είτε για δημόσιους. Άλλωστε γι' αυτό και η εφαρμογή του προγραμματίστηκε έναν χρόνο μετά την ψήφισή του.

Αναμφίβολα, η χώρα μας όφειλε να είχε προετοιμαστεί έγκαιρα ώστε να αντιμετωπίσει επαρκώς τις αυξανόμενες απαιτήσεις που επιβάλλονται από τις ρυθμίσεις του Γενικού Κανονισμού. Όφειλε από την αρχή της ψήφισης του Κανονισμού το 2016 να είχε ενημερώσει όλες τις επιχειρήσεις που λόγω αντικειμένου, επηρεάζονται από τον Κανονισμό, καθώς και να κάνει πιο κατανοητή την έννοια του «ευαίσθητου δεδομένου». Έτσι θα είχαν αποφευχθεί καταστάσεις σύγχυσης και πανικού που παρατηρήθηκαν, κυρίως λόγω της άγνοιας και της επιβολής των υψηλών προστίμων που ορίζει ο Κανονισμός σε περίπτωση λάθους.

Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί, οι περισσότερες επιχειρήσεις δεν είναι ακόμα έτοιμες να υποδεχθούν και να συμμορφωθούν με τον GDPR, είτε λόγω αντίδρασής τους στο νέο Κανονισμό, είτε λόγω μη επαρκούς ενημέρωσής τους για τον τρόπο εφαρμογής του. Ακόμη, στελέχη του δημόσιου τομέα αναφέρουν ότι μετρώνται στα δάκτυλα του ενός χεριού οι φορείς που έχουν ορίσει υπεύθυνο προστασίας προσωπικών δεδομένων (DPO). Ούτε καν η ΓΓ 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. Στελέχη της ανέφεραν ότι το θέμα της εφαρμογής του GDPR θα την απασχολήσει μετά την 25η Μαΐου. Εξίσου κρίσιμος τομέας είναι εκείνος της υγείας (νοσοκομεία, φαρμακευτικές εταιρίες κ.λπ.). 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.

Για το λόγο αυτό, προτάθηκαν τα βασικά βήματα προετοιμασίας και οι μεθοδολογίες που μπορούν να βοηθήσουν μια επιχείρηση στην ομαλότερη μετάβαση στον GDPR. Αυτά σχετίζονται με την κατανόηση του Κανονισμού και την αναγνώριση του είδους των προσωπικών δεδομένων που έχει στην κατοχή της η επιχείρηση, την ανίχνευση και την αξιολόγηση των συστημάτων και των δικλείδων ασφαλείας που παρέχει στους πελάτες της για την προστασία των δεδομένων τους,

τον ορισμό του DPO, την αναδιοργάνωση των εσωτερικών της λειτουργιών και πληροφοριακών υποδομών της, τη συνεχή εκπαίδευση του προσωπικού της και το σχεδιασμό και την υλοποίηση μιας ολοκληρωμένης στρατηγικής που θα οδηγήσει στη συμμόρφωση με τον GDPR.

Αρκετοί, πάντως, οργανισμοί του ιδιωτικού τομέα, και κυρίως οι θυγατρικές πολυεθνικών ομίλων, συμμορφώνονται προς τη νέα οδηγία, ενώ τους τελευταίους μήνες οι Έλληνες καταναλωτές 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, το 69% των επιχειρήσεων στην Ελλάδα δεν είναι ενημερωμένες για τον νέο κανονισμό.

Η παραπάνω δήλωση της συμμόρφωσης των οντοτήτων στον ιδιωτικό τομέα, επιβεβαιώνεται και με την μελέτη των δύο περιπτώσεων που εξετάστηκαν στην παρούσα διπλωματική εργασία. Διαπιστώθηκε ότι τόσο στην φαρμακευτική εταιρία , όσο και στη Τράπεζα, αν και σε μικρότερο βαθμό, η εφαρμογή της μεθοδολογίας συμμόρφωσης με τον Κανονισμό σε θεωρητικό υπόβαθρο, συγκλίνει και με την πρακτική εφαρμογή του στην ελληνική πραγματικότητα. Η φαρμακευτική εταιρεία έκανε αποτελεσματική χρήση των μεθοδολογιών και των πρακτικών που περιέγραψε η παρούσα διπλωματική εργασία, και πλέον είναι σε θέση να προχωρήσει στα επόμενα βήματα συμμόρφωσης με τον κανονισμό, καθώς και να επαναπροσδιορίσει τις μεθόδους και τις τεχνικές που χρησιμοποιεί για την προστασία και ασφάλεια προσωπικών δεδομένων που διαχειρίζεται. Η γενική ιδέα της προετοιμασίας και ανίχνευσης των δεδομένων, της αξιολόγησης και εκτίμησης αυτών και της υλοποίησης της στρατηγικής παραμένουν ίδια, ενώ μεγάλο αντίκτυπο για την πραγματοποίηση όλων αυτών έχει η διαμόρφωση μιας ενιαίας κουλτούρας στις εσωτερικές λειτουργίες της επιχείρησης.

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, ενώ είναι αρμόδιος και 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.

Το ανθρώπινο δυναμικό, οφείλει να ενημερώνεται και να εκπαιδεύεται συνεχώς σχετικά με τον υπάρχοντα Κανονισμό, ή με τυχόν τροποποιήσεις του. Όπως έγινε αντιληπτό και από την μελέτη των δύο περιπτώσεων, η εκπαίδευση αποτελεί ένα σημαντικό πυλώνα συμμόρφωσης με τον GDPR αλλά και καλύτερης γνώσης του τόσο από τους υπεύθυνους προστασίας δεδομένων, όσο και από το ανθρώπινο δυναμικό της εκάστοτε οντότητας. Έτσι ο υπάλληλος βρίσκεται σε συνεχή ετοιμότητα για τυχόν μελλοντικές παραβιάσεις ή έκτακτες καταστάσεις που μπορεί να προκύψουν. Οι ιθύνοντες των εταιριών θα πρέπει να προβαίνουν συχνά σε διοργάνωση ειδικών σεμιναρίων, workshops ή συνεδρίων σχετικά με τον GDPR και των τελευταίων εξελίξεων γύρω από το θέμα, ούτως ώστε να επιτυγχάνεται η εύρυθμη λειτουργία της οντότητας, και φυσικά να αποφεύγεται η επιβολή υψηλών προστίμων.

Κλείνοντας, καταλήγουμε στο συμπέρασμα πως ο νέος αυτός Κανονισμός είναι ένα σημαντικό «εργαλείο», που θα ενισχύσει την αξιοπιστία της Ηλεκτρονικής Διακυβέρνησης, συνεπώς και την εμπιστοσύνη των πολιτών προς αυτήν, ώστε να δημιουργηθούν οι προϋποθέσεις για προσφορά ποιοτικότερων υπηρεσιών από τη Δημόσια Διοίκηση αλλά και από τις ιδιωτικές οικονομικές οντότητες. Θεωρούμε πως η εγκαθίδρυση της εμπιστοσύνης που έχει φέρει η εφαρμογή του Γενικού Κανονισμού θα αποτελέσει στο άμεσο μέλλον σημαντικό βήμα βελτίωσης των ίδιων των φορέων και επιχειρήσεων σε μια σύγχρονη «αγορά».

Η εφαρμογή του Γενικού Κανονισμού, θα συμβάλει αποφασιστικά στην ενίσχυση του πέπλου προστασίας των προσωπικών δεδομένων των φυσικών προσώπων και θα ισχυροποιήσει τη θέση τους, είτε στον τομέα της συναλλαγής τους με δημόσιους φορείς και οργανισμούς και στον ρόλο τους ως «διοικούμενοι», είτε όσον αφορά τον τομέα της συναλλαγής τους με επιχειρήσεις ή άλλους ιδιωτικούς φορείς και οντότητες. Ακόμη θα συμβάλει στην ομοιογενοποίηση και βελτίωση των συνθηκών ανταγωνισμού εντός της Ένωσης.

Ωστόσο, αν εξαιρέσουμε τις περιπτώσεις της Τράπεζας και της φαρμακευτικής εταιρείας, είναι νωρίς ακόμα, παρότι ο νόμος έχει τεθεί σε ισχύ εδώ και 6 περίπου μήνες, να εξάγουμε ασφαλή συμπεράσματα ότι όλες οι οικονομικές οντότητες

δημόσιες ή ιδιωτικές έχουν συμμορφωθεί με τους κανόνες και τις διατάξεις που ορίζει ο GDPR. Ας μην ξεχνάμε πως ειδικά στη χώρα μας, η εφαρμογή και υλοποίηση νόμων, χρειάζεται ένα αρκετά μεγάλο διάστημα για να εφαρμοστούν, αφού απουσιάζουν οι έλεγχοι και η επιβολή προστίμων, που θα αφυπνίσουν τον Έλληνα επιχειρηματία αλλά και τους ιθύνοντες δημόσιων οργανισμών ώστε να εφαρμόσουν τα όσα ορίζονται.

8.2 Περιορισμοί στην Έρευνα

Κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας, συναντήθηκαν αρκετά προβλήματα όσον αφορά την συλλογή πληροφοριών. Επειδή ο Κανονισμός αυτός, έχει πρόσφατα εισέλθει στη χώρα μας, το υλικό που είναι διαθέσιμο είναι αρκετά περιοριορισμένο. Παρότι πραγματοποιήθηκε επικοινωνία με αρκετούς οργανισμούς δημόσιους και ιδιωτικούς, εν τούτοις η απάντηση στην χορήγηση επιπρόσθετου υλικού ήταν αρνητική. Είναι γνωστό πως στις μέρες μας, ο ανταγωνισμός μεταξύ των οικονομικών οντοτήτων, είναι μεγάλος και πολλοί από τους οργανισμούς αρνούνται να παρέχουν υλικό, φοβούμενοι τον κίνδυνο της «αντιγραφής» της στρατηγικής τους, ειδικά σε κάτι που είναι πρωτόγνωρο για τις επιχειρήσεις, όπως ο νέος Κανονισμός του GDPR.

8.3 Προτάσεις για περαιτέρω Έρευνα

Η συμβολή των αποτελεσμάτων της έρευνας αυτής, μπορεί να αποτελέσει κίνητρο για περαιτέρω έρευνα σχετικά με τον έλεγχο της καθολικής εφαρμογής του Κανονισμού από όλες τις δημόσιες ή ιδιωτικές οικονομικές οντότητες. Θα μπορούσε επίσης να γίνει μια συγκριτική ανάλυση μεταξύ των εταιριών που εφάρμοσαν τον Κανονισμό στην χώρα μας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

Carey , P. (2018). *Fifth Edition data protection "A practical quide to UK and EU law"* . United Kingdom : Odxord University Press.

Lambrinoudakis, C. (2018). *The General Data Protection Requlation (GDPR) Era"Ten steps gor compiance of Data processors and Data conrollers. In: Furnell S.,Mouratidis H. Pernul G. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2018. Lecture Notes in Computer Science,vol 11033. Springer,Cham*

Gartner, (2017) Six steps to PSD2-Digital banking Reimagined in Europe and Beyond. (https://www.gartner.com/doc/3773968/steps-psd--digital-banking

Voigt , P., & Bussche , A. (2017). *The EU General Data Protection Regulation (GDPR) "A practical quide".* Berlin-Hamburg Germany: Springer International Publishing.

Ιγγλεζάκης, Ι. (2004). *Ευαίσθητα προσωπικά δεδομένα.* Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

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

Μήτρου , Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων* . Αθήνα : Εκδόσεις Σάκκουλα .

Σωτηρόπουλος , Β. (2006). *Η Συνταγματική προστασία των προσωπικών δεδομένων.* Αθήνα-Θεσσαλονίκη : Εκδόσεις Σάκκουλα .

Σωτηρόπουλος , Β. (2017). *Υπεύθυνος προστασίας δεδομένων. "εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδωτικό τομέα".* Αθήνα-Θεσσαλονίκη : Εκδόσεις Σάκκουλα.

ΕΠΙΣΤΗΜΟΝΙΚΑ ΑΡΘΡΑ-ΠΑΡΟΥΣΙΑΣΕΙΣ

Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute (2015): 2015 Cost of Data Breach Study: Global Analysis

GDPR: Χρήσιμες Συμβουλές για όσες επιχειρήσεις δεν έχουν ξεκινήσει ακόμα. (Ετήσια έκδοση 2017). *Netweek: "A Practical quide to GDPR"* .

http://www.businessnews.gr/article/91283/wind-oloklirose-ergo-eu-gdpr-me-tehnologies-oracle. (2017, Νοέμβριος 14). Wind: Ολοκλήρωσε έργο EU GDPR με τεχνολογίες Oracle .

Oracle Απαραίτητη η ξεκάθαρη στρατηγική it ασφαλείας για τη συμμόρφωση με τον GDPR . (Ετήσια Έκδοση 2017). *Netweek A practical quide to GDPR*.

Vordos, I. I. (2017). *"Preparing for Compliance with GDPR-Backround and Solutions"*.

Wyman, O.,Ivell, T.,Wilkinson, B., Helps, B. (2017). Future proofing privacy:GDPR compliance in a networked Banking system. Point of view

Καλαντζής , Π. (Ετήσια έκδοση 2017). Στρατηγική Συμμόρφωσης με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων. *Netweek "A Practical Guide to GDPR"* .

Ομάδα εργασίας του ΣΕΒ για τα προσωπικά δεδομένα, (Οκτώβριος 2018), Ο νέος Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR):"εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης", Αθήνα

Παναγοπούλου , Φ. (2017). *Τα νέα δικαιώματα για τους πολίτες βάσει του Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση.*

Σιασιάκος , Κ., Αναστασίου , Σ., & Τούντας , Κ. (2016). *Εκτίμηση των επιπτώσεων σχετικά με την Προστασία των Προσωπικών Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης* .

ΝΟΜΟΙ-ΚΑΝΟΝΙΣΜΟΙ

Νόμος 2472/1997 (ΦΕΚ Α’ 50/10.4.1997), Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις.

Νόμος 3471/2006 (ΦΕΚ Α’ 133/28-06-2006) Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Νόμος 3917/2011 (ΦΕΚ Α’ 22/21-02-2011) Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

Νόμος 4070/2012 (ΦΕΚ Α’ 82/10-04-2012) Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.

Νόμος (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending

Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα http://www.dpa.gr/

ARTICLE 29 DATA PROTECTION WORKING PARTY, Adopted on 8 June 2017 Διαθέσιμο στη διεύθυνση: file:///C:/Users/Ergo/Downloads/Opinion22017ondataprocessingatwork-wp249.pdf

PSD2 - the directive that will change banking as we know it https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/

https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2577380

https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/risk/dt_mt_risk_gdpr_privacy_services_brochure.pdf

https://www.icap.gr (ICAP Management Consultants), Φεβρουάριος 2018

https://www.rsm.global/ireland/sites/default/files/media/gdpr_roadmap_to_compliance_printable_version_-_terry_mcadam.pdf

https://www.pwc.com/gdpr

https://www.priority.com.gr/software/

https://www.bankinghub.eu/banking/finance-risk/general-data-protection-regulation

https://www.oracle.com/applications/gdpr/

Wind: Ολοκλήρωσε έργο EU GDPR με τεχνολογίες Oracle: http://www.businessnews.gr/article/91283/wind-oloklirose-ergo-eu-gdpr-me-tehnologies-oracle

www.algosystems.gr «GDPR, ALGOSYSTEMS και PRIORITY. It’s time to meet your GPDR Challenge!»

https://www.weforum.org (WORLD ECONOMIC FORUM)