



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΔΠΜΣ ΣΤΗΝ «ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ»
ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
ΣΤΙΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ
(THE PROTECTION OF PERSONAL DATA IN
SMALL AND MEDIUM-SIZED ENTERPRISES)

Φοιτήτρια: Καλλιώρα Αικατερίνη του Παναγιώτη
Επιβλέπουσα καθηγήτρια: Καραγκούνη Γλυκερία

ΛΑΡΙΣΑ

ΟΚΤΩΒΡΙΟΣ, 2024

Υπεύθυνη δήλωση:

Βεβαιώνω ότι είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στη διπλωματική εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Τέλος, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά για τις απαιτήσεις του ΔΠΜΣ Επιχειρηματικότητας.

Λάρισα, 10/10/2024

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την καθηγήτρια μου Καραγκούνη Γλυκερία, για όλη τη υποστήριξη, που μου παρείχε κατά τη διάρκεια της εκπόνησης αυτής της εργασίας. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου, που στέκεται αρωγός σε κάθε βήμα της ζωής μου.

Πίνακας περιεχομένων

Περίληψη.....	5
Abstract	6
Συντομογραφίες.....	7
Εισαγωγή.....	8
1. Θεωρητική θεμελίωση της εμφάνισης και εξέλιξης των προσωπικών δεδομένων στο ενωσιακό και εθνικό δίκαιο	10
1.1. Προγενέστερα νομοθετήματα στο ενωσιακό δίκαιο	10
1.2. Ν. 2472/1997	14
2. Η ψήφιση του Κανονισμού 2016/679-GDPR για την προστασία των προσωπικών δεδομένων.....	16
2.1. Ν. 4624/2019	18
2.2. Όργανα για την προστασία των προσωπικών δεδομένων	19
3. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων στις επιχειρήσεις ...	22
3.1. Τα GDPR στις μικρές και μικρομεσαίες επιχειρήσεις.....	25
3.2. Τα GDPR και η εφαρμογή τους από τα πιστωτικά ιδρύματα.....	28
3.3. Εφαρμογή της προστασίας προσωπικών δεδομένων – Μελέτη περίπτωσης οι μεσαίες και μικρομεσαίες επιχειρήσεις	30
4. Ερευνητικό μέρος	35
4.1. Ερευνητικός σκοπός.....	35
4.3. Ερευνητικό εργαλείο.....	35
4.4. Ερευνητικό δείγμα	37
4.5. Αποτελέσματα έρευνας - Συζήτηση.....	39
5. Συμπεράσματα – Προτάσεις.....	48
ΠΑΡΑΡΤΗΜΑ Ι (ΟΔΗΓΟΣ ΣΥΝΕΝΤΕΥΞΗΣ)	51
Βιβλιογραφία.....	54

Περίληψη

Αντικείμενο της παρούσας διπλωματικής αποτελεί η προστασία προσωπικών δεδομένων στις μικρομεσαίες επιχειρήσεις. Στο πρώτο κεφάλαιο αναλύεται η εμφάνιση και εξέλιξη των προσωπικών δεδομένων στο ενωσιακό και εθνικό δίκαιο, μέσω της αναδρομής στα προϊσχύσαντα νομοθετικά κείμενα. Στο δεύτερο κεφάλαιο πραγματοποιείται ανάλυση του Κανονισμού 2016/697 – GDPR, του Ν. 4624/2019 μέσω του οποίου θεσπίστηκαν κανόνες εντός της ελληνικής επικράτειας, οι οποίοι σχετίζονται με τον Νέο Κανονισμό, καθώς και των οργάνων που προασπίζουν την προστασία των προσωπικών δεδομένων. Στο τρίτο κεφάλαιο ακολουθεί η εφαρμογή του Γενικού Κανονισμού για την Προστασία Προσωπικών Δεδομένων στις επιχειρήσεις γενικά, καθώς και στις μικρομεσαίες επιχειρήσεις και στα πιστωτικά ιδρύματα, μελετώντας περιπτώσεις μικρών και μεσαίων επιχειρήσεων, οι οποίες δραστηριοποιούνται σε χώρες εντός της Ευρωπαϊκής Ένωσης. Στο τέταρτο κεφάλαιο ακολουθεί η πραγματοποίηση της έρευνας, προκειμένου να διερευνηθούν τα ερευνητικά ερωτήματα, χρησιμοποιώντας ως ερευνητικό εργαλείο την συνέντευξη και ως ερευνητικό δείγμα 10 μικρομεσαίες επιχειρήσεις της Περιφέρειας Θεσσαλίας και Στερεάς Ελλάδας. Κλείνοντας, αποτυπώνονται κρίσεις και συμπεράσματα από την εφαρμογή του Κανονισμού στις μικρομεσαίες επιχειρήσεις και προτείνεται η περαιτέρω έρευνα και εμβάθυνση σε ευρύτερο πεδίο εντός της επικράτειας.

Λέξεις-Κλειδιά: GDPR, προστασία προσωπικών δεδομένων, μικρομεσαίες επιχειρήσεις, συμμόρφωση, Κανονισμός

Abstract

The subject of this thesis is the protection of personal data in small and medium-sized enterprises. The first chapter analyses the emergence and evolution of personal data in EU and national law, by reviewing the previous legislative texts. The second chapter analyses Regulation 2016/697 - GDPR, Law 4624/2019 through which rules were adopted within the Greek territory, which are related to the New Regulation, as well as the institutions that uphold the protection of personal data. The third chapter follows the application of the General Data Protection Regulation to businesses in general, as well as to small and medium-sized enterprises and credit institutions, studying cases of small and medium-sized enterprises operating in countries within the European Union. In chapter four follows the implementation of the research in order to investigate the research questions, using interviews as a research tool and 10 small and medium-sized enterprises of the Region of Thessaly and Central Greece as a research sample. In conclusion, judgments and conclusions from the implementation of the Regulation in SMEs are reflected and further research and deepening in a wider field within the territory is proposed.

Keywords: GDPR, personal data protection, small and medium-sized enterprises, compliance, Regulation

Συντομογραφίες

ΑΕΙ	Ανώτατο Εκπαιδευτικό Ίδρυμα
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
Ε.Ε.	Ευρωπαϊκή Ένωση
Ε.Κ.	Ευρωπαϊκό Κοινοβούλιο
Ν.	Νόμος
ΣΛΕΕ	Συνθήκη για την Λειτουργία της Ευρωπαϊκής Ένωσης
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
ΧΘΔ	Χάρτης Θεμελιωδών Δικαιωμάτων

DPO	Data Protection Officer
GDPR	General Data Protection Regulation

Εισαγωγή

Οι πληροφορίες που αποτελούν προσωπικά δεδομένα δεν επιτρέπεται να κοινοποιούνται ελεύθερα ή να διαβιβάζονται σε τρίτους δίχως την συγκατάθεση του προσώπου που αφορούν. Ειδικότερα, *«η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα»*. Συνεπώς, κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Σύμφωνα με τον ΓΚΠΔ, ως δεδομένα προσωπικού χαρακτήρα θεωρούνται *«κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (»υποκείμενο των δεδομένων«)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»*.

Ως επεξεργασία νοείται *«κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή»*.

Τα νέα δεδομένα της εποχής δημιούργησαν την ανάγκη προσαρμογής του τρόπου προστασίας των προσωπικών δεδομένων. Ειδικότερα, η συνεχής τεχνολογική ανάπτυξη, σε συνδυασμό με την παγκοσμιοποίηση τροποποίησαν τα δεδομένα της οικονομικής και κοινωνικής ζωής και μεγιστοποίησαν τον όγκο δεδομένων προσωπικού χαρακτήρα που συλλέγονται και ανταλλάσσονται. Κατ' επέκταση, και οι ιδιωτικές επιχειρήσεις, αλλά και οι δημόσιες αρχές προκειμένου να επιτύχουν το σκοπό της δραστηριοποίησής τους, χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα σε μεγαλύτερο όμως όγκο. Επιπλέον και τα ίδια τα φυσικά πρόσωπα προκειμένου να συμβαδίσουν με τα νέα δεδομένα της εποχής

δημοσιοποιούν περισσότερες πληροφορίες που αφορούν τους ίδιους και τις καθιστούν δημόσια προσβάσιμες.

Ειδικότερα, όσον αφορά τις επιχειρήσεις, αυτές προσπαθούν να αποκτήσουν μεγαλύτερη πρόσβαση στα προσωπικά δεδομένα των καταναλωτών τους, προκειμένου να εξειδικεύουν και εξατομικεύουν τις παροχές τους, ώστε να ικανοποιούν όλους τους εν δυνάμει πελάτες τους.

Τα ανωτέρω καθιστούν αναγκαία την δημιουργία και εφαρμογή ενός αυστηρού νομοθετικού πλαισίου, το οποίο και θα εμπνέει εμπιστοσύνη στα φυσικά πρόσωπα, αλλά και θα συμβάλλει στην ανάπτυξη της ψηφιακής οικονομίας και του ηλεκτρονικού εμπορίου. Για το λόγο αυτό ψηφίστηκε ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο οποίος έχει εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, ως ένα ομοιόμορφο και ισοδύναμο πεδίο στην προστασία των προσωπικών δεδομένων. Αναδύεται επομένως η ανάγκη ισχύς του Κανονισμού, ο οποίος διασφαλίζει την ασφάλεια δικαίου και την διαφάνεια, και στις επιχειρήσεις, συμπεριλαμβάνοντας τις πολύ μικρές, τις μικρές και τις μεσαίες επιχειρήσεις.

1. Θεωρητική θεμελίωση της εμφάνισης και εξέλιξης των προσωπικών δεδομένων στο ενωσιακό και εθνικό δίκαιο

1.1. Προγενέστερα νομοθετήματα στο ενωσιακό δίκαιο

Θα πραγματοποιηθεί βιβλιογραφική ανασκόπηση, σύμφωνα με την οποία θα αποτυπωθεί ο τρόπος εμφάνισης και εξέλιξης των προσωπικών δεδομένων στο ενωσιακό δίκαιο. Σύμφωνα με τον Τζώρτζη, στην Ευρωπαϊκή Ένωση εφαρμόζονται νομοθετικά κείμενα, τα οποία έχουν σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα. Με την Συνθήκη του Μάαστριχτ καθιερώθηκαν νέοι πυλώνες, οι οποίοι κατακερμάτισαν την τότε ισχύουσα νομοθεσία, η οποία κρίθηκε ανεπαρκής. Έως τα μέσα του 1990, τα μη εναρμονισμένα δίκαια των κρατών μελών ρύθμιζαν τα δεδομένα προσωπικού χαρακτήρα και τη προστασία αυτών.

Σύμφωνα με την Europa (2014), η Οδηγία 1995/46 ΕΚ αποτελεί σημείο αναφοράς για την προστασία προσωπικών δεδομένων. Ειδικότερα, εκδόθηκε στις 24 Οκτωβρίου 1995 από το Ευρωπαϊκό Κοινοβούλιο και εγκαινιάζει την προστασία που αφορά τα φυσικά πρόσωπα σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, καθώς και την ελεύθερη κυκλοφορία των δεδομένων. Η εφαρμογή της γίνεται κυρίως στα δεδομένα, τα οποία χρήζουν επεξεργασίας με διαδικασία, η οποία είναι αυτοματοποιημένη, αλλά και την μη αυτοματοποιημένη επεξεργασία, η οποία αφορά τα προσωπικά δεδομένα που επίκειται να περιληφθούν σε αρχείο, όπως είναι και αυτά που αποτυπώνονται παραδοσιακά στο χαρτί.

Η Οδηγία δεν έχει εφαρμογή όταν αφορά επεξεργασία προσωπικών δεδομένων κατά τις προσωπικές ή οικιακές δραστηριότητες, καθώς και όταν αφορούν δραστηριότητες, οι οποίες δεν εμπίπτουν στο κοινοτικό δίκαιο, όπως είναι η δημόσια ασφάλεια, η άμυνα ή η ασφάλεια του κράτους. Σύμφωνα με την Οδηγία, κρίνεται νόμιμο να επεξεργάζονται δεδομένα 1) όταν υπάρχει συγκατάθεση του προσώπου που αφορά, 2) όταν είναι απαραίτητη για την εκτέλεση της σύμβασης, όπου το πρόσωπο που αφορά είναι συμβαλλόμενος, 3) όταν κρίνονται απαραίτητα από τον υπεύθυνο επεξεργασίας, λόγω υποχρεωτικότητας του νόμου, 4) όταν διαφυλάσσονται συμφέροντα ζωτικής σημασίας για το πρόσωπο που αφορούν, 5) όταν εμπίπτουν στο πλαίσιο εκπλήρωσης έργων δημόσιου συμφέροντος ή στην άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας και 6) όταν είναι αναγκαίο για να επιτευχθεί το έννομο συμφέρον, το οποίο επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος,

με την προϋπόθεση της αρχής της αναλογικότητας σε σχέση με τα δεδομένα που προστατεύονται.

Τα παραπάνω αποτελούν γενικές αρχές ποιότητας των δεδομένων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων. Αυτές οι αρχές συνήθως αντανakλούν τις βασικές αρχές του κανονιστικού πλαισίου για την προστασία των δεδομένων, όπως και του Γενικού Κανονισμού (GDPR) στην Ευρωπαϊκή Ένωση.

Περαιτέρω η Οδηγία προκρίνει την τήρηση ορισμένων αρχών σχετικά με την νομιμοποίηση των δραστηριοτήτων που σχετίζονται με την επεξεργασία δεδομένων. Ειδικότερα: i) Νόμιμη και Δίκαιη Επεξεργασία: Η επεξεργασία προσωπικών δεδομένων πρέπει να βασίζεται σε σαφείς, νόμιμους και θεμιτούς σκοπούς. Η συλλογή προσωπικών δεδομένων πρέπει να γίνεται με ενημέρωση και συγκατάθεση του ατόμου που αφορούν, ii) Περιορισμένη Επεξεργασία: Τα δεδομένα πρέπει να συλλέγονται για συγκεκριμένους και νόμιμους σκοπούς και δεν πρέπει να χρησιμοποιούνται για άλλους σκοπούς πέραν αυτών. Επίσης, πρέπει να αποθηκεύονται μόνο για το χρονικό διάστημα που είναι απαραίτητο για τον επιδιωκόμενο σκοπό, iii) Ειδικές Κατηγορίες Δεδομένων: Η επεξεργασία ευαίσθητων κατηγοριών δεδομένων (όπως φυλετική καταγωγή, θρησκευτικές πεποιθήσεις, υγεία) είναι περιορισμένη και απαιτεί ειδικούς λόγους, όπως συγκατάθεση, υπεράσπιση ζωτικών συμφερόντων, ιατρική διάγνωση, ή άσκηση νομικών δικαιωμάτων.

Αυτές οι αρχές βοηθούν στη διασφάλιση ότι η επεξεργασία προσωπικών δεδομένων πληροί υψηλά πρότυπα προστασίας και δεν παραβιάζει τα δικαιώματα των ατόμων που αφορά.

Το ενδιαφερόμενο πρόσωπο, του οποίου τα δεδομένα υποβάλλονται σε επεξεργασία, έχει σημαντικά δικαιώματα για την προστασία των προσωπικών του δεδομένων, όπως αναφέρονται στο πλαίσιο της νομοθεσίας περί προστασίας δεδομένων. Τα βασικά δικαιώματα αυτά περιλαμβάνουν: **α) Δικαίωμα Ενημέρωσης (Πληροφόρησης)**: Το ενδιαφερόμενο πρόσωπο έχει το δικαίωμα να ενημερωθεί για την επεξεργασία των προσωπικών του δεδομένων, συμπεριλαμβανομένων του υπεύθυνου επεξεργασίας, των σκοπών της επεξεργασίας, των κατηγοριών των δεδομένων, και των παραληπτών, **β) Δικαίωμα Πρόσβασης**: Το άτομο έχει το δικαίωμα να ζητήσει και να λάβει πρόσβαση στα προσωπικά του δεδομένα που υφίστανται επεξεργασία, καθώς και πληροφορίες σχετικά με την επεξεργασία αυτή, **γ) Δικαίωμα Αντίρρησης (Αντιταξικότητας)**: Το άτομο έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των προσωπικών του δεδομένων για νόμιμους λόγους που το

αφορούν. Σε ορισμένες περιπτώσεις, όπως η διαφήμιση, μπορεί να αντιταχθεί και να αποτρέψει την επεξεργασία των δεδομένων του για αυτούς τους σκοπούς, **δ) Δικαίωμα Νομικής Προσφυγής:** Το άτομο έχει το δικαίωμα να ασκήσει νομική προσφυγή σε περίπτωση παραβίασης των δικαιωμάτων του στον τομέα της προστασίας δεδομένων.

Επιπλέον, η παρέμβαση των ελεγκτικών αρχών και η διασφάλιση της εμπιστευτικότητας και ασφάλειας της επεξεργασίας αποτελούν σημαντικά στοιχεία για την προστασία των προσωπικών δεδομένων. Επιπλέον, η επικοινωνία ανάμεσα στα κράτη μέλη και η συνεργασία σε επίπεδο Ευρωπαϊκής Ένωσης συμβάλλουν στην ενιαία εφαρμογή των προτύπων προστασίας δεδομένων.

Με την ανωτέρω Οδηγία θεσπίζεται για πρώτη φορά το κανονιστικό πλαίσιο, με το οποίο γίνεται προσπάθεια εξισορρόπησης της προστασίας της ιδιωτικής ζωής των φυσικών προσώπων με την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης. Η υιοθέτηση της Οδηγίας από τα κράτη μέλη της Ένωσης ήταν απαραίτητη, προκειμένου να επιλυθεί το ζήτημα της ισχύος διαφορετικών νομοθετικών ρυθμίσεων από κράτος μέλος σε κράτος μέλος και να δημιουργηθεί ένα ενιαίο πλαίσιο σχετικά με την ελεύθερη κυκλοφορία των δεδομένων.

Για την υλοποίηση των ανωτέρω, η Ευρωπαϊκή Ένωση μέσω της Οδηγίας οριοθετεί το πλαίσιο για τα προσωπικά δεδομένα προσωπικού χαρακτήρα, ζητώντας από το κάθε κράτος μέλος να τηρεί τα θεσπιζόμενα μέτρα και παράλληλα να δημιουργήσει έναν ανεξάρτητο εθνικό οργανισμό, ο οποίος θα επιφορτίζεται με την εποπτεία των δραστηριοτήτων που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Επιπλέον, μέσω της Συνθήκης της Λισαβόνας υπήρξε αναβάθμιση του δικαιώματος της προστασίας προσωπικών δεδομένων στο ενωσιακό δίκαιο, κατοχυρώνοντας το δικαίωμα της προστασίας προσωπικών δεδομένων, μέσω του άρθρου 16 παρ. 1 ΣΛΕΕ, καθώς και με τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, όπου σύμφωνα με το άρθρο 8 «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 συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.». Με το ανωτέρω άρθρο του Χάρτη, πραγματοποιήθηκε ολιστική ρύθμιση τόσο των αρχών που

συνοδεύουν τα προσωπικά δεδομένα, όσο και περαιτέρω ζητημάτων που σχετίζονται με αυτά και τον έλεγχο τους.

Με βάση τα δεδομένα που έχουν συλλεχθεί μέσω της Europa (2014), γίνεται αντιληπτό ότι υπήρξε αύξηση στην διαβίβαση των δεδομένων των ανθρώπων, η οποία δημιούργησε την ανάγκη για πληρέστερη προστασία και συμπεριλάμβανε και τις ηλεκτρονικές επικοινωνίες, που άρχισαν να εμφανίζονται και να επηρεάζουν την ιδιωτική ζωή των ανθρώπων. Για το λόγο αυτό, στις 12 Ιουλίου 2002 εκδόθηκε η Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, η οποία αφορούσε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Η νέα Οδηγία αποτελεί συμπληρωματική της προϋπάρχουσας Οδηγίας 95/46/EK, χωρίς όμως να την καταργεί, εξειδικεύοντας τους σκοπούς της και προσθέτοντας ειδικές ρυθμίσεις για τις ηλεκτρονικές επικοινωνίες. Επιπλέον, στο άρθρο 3 της Οδηγίας εισήχθησαν και νέοι ορισμοί, οι οποίοι θα ακολουθούν τις διατάξεις σχετικά με τα προσωπικά δεδομένα. Ειδικότερα: α) «χρήστης», κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας· β) «δεδομένα κίνησης», τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της· γ) «δεδομένα θέσης», τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών· δ) «επικοινωνία», κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες μπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει· ε) «κλήση», σύνδεση που πραγματοποιείται μέσω μιας διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας που επιτρέπει αμφίδρομη επικοινωνία σε πραγματικό χρόνο· στ) «συγκατάθεση» του χρήστη ή του συνδρομητή, η συγκατάθεση του προσώπου που αφορούν τα δεδομένα, κατά την έννοια της οδηγίας 95/46/EK· ζ) «υπηρεσία προστιθέμενης αξίας», κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση μιας

επικοινωνίας και τη χρέωσή της · η) «ηλεκτρονικό ταχυδρομείο», κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη έως ότου ληφθεί από τον παραλήπτη.

Με βάση την νέα αυτή Οδηγία (2002), η ισχύς της επεκτείνεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά την παροχή των διαθέσιμων υπηρεσιών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας, λόγω των νέων προηγμένων ψηφιακών τεχνολογιών στα δημόσια δίκτυα επικοινωνίας. Μετά την καθιέρωση νέων υπηρεσιών κατά την χρήση των ηλεκτρονικών επικοινωνιών και την πιο προσιτή και οικονομική προσβασιμότητα στα ψηφιακά κινητά δίκτυα, η μεταρρύθμιση των προηγούμενων διατάξεων ήταν μονόδρομος, προκειμένου να μπορεί να συμβαδίζει με την νέα πραγματικότητα που είχε διαμορφωθεί.

Με τις ανωτέρω ρυθμίσεις πραγματοποιήθηκε μία σημαντική προσπάθεια να διασφαλιστούν τα δικαιώματα των ατόμων σε ευρωπαϊκό επίπεδο και στην συνέχεια να μεταφερθεί το πλαίσιο αυτό και σε όλα τα έθνη. Η προσαρμογή όμως αυτή γίνονταν με σημαντικές διαφοροποιήσεις από κράτος σε κράτος, λόγω της μεγάλης διακριτικής ευχέρειας που υπήρχε για την εφαρμογή τους από την Οδηγία, με αποτέλεσμα να υπάρχει μεγάλη απόκλιση κατά την εναρμόνιση με την Οδηγία, η οποία ανέδυσσε και έντονους προβληματισμούς για την αποτελεσματική ισχύ και την εφαρμογή της Οδηγίας.

1.2. Ν. 2472/1997

Στο σημείο αυτό είναι απαραίτητη η βιβλιογραφική ανασκόπηση, ώστε να γίνει αντιληπτός ο τρόπος μεταφοράς της Οδηγίας εντός της Ελλάδος. Ειδικότερα, σύμφωνα με τον Ιγγλεζάκη (2020), μέσω του Ν. 2472/1997 έγινε μεταφορά της Οδηγίας 1995/46 ΕΚ στην ελληνική επικράτεια. Τα προσωπικά δεδομένα και η προστασία αυτών ξεκίνησαν να υφίστανται στον ελλαδικό χώρο αυτοτελώς τα τελευταία τριάντα έτη, λόγω ανεπάρκειας που παρατηρήθηκε στο Δίκαιο προστασίας. Ειδικότερα, μέσω του Συντάγματος του 1975, υπήρξε κατοχύρωση της ιδιωτικής οικογενειακής ζωής, χωρίς όμως να προβλέπεται οποιαδήποτε ρύθμιση σχετικά με την προστασία των προσωπικών δεδομένων. Η μοναδική ρύθμιση που προϋπήρχε και στην οποία θα μπορούσε να βασιστεί η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι οι διατάξεις σεβασμού της αξίας του ανθρώπου (άρθρ. 2 παρ. 1 Σ) και της ελεύθερης ανάπτυξης της προσωπικότητας (άρθρ. 5 Σ).

Η μεταφορά της Οδηγίας στην ελληνική επικράτεια επέφερε την συνταγματική κατοχύρωση της προστασίας των δεδομένων με την προσθήκη του άρθρο 9^Α του Συντάγματος, κατά την αναθεώρηση του έτους 2001. Με βάση την Οδηγία 95/46/EK, όπως και των ανωτέρω ρυθμίσεων που ακολούθησαν, πραγματοποιήθηκε η προάσπιση των προσωπικών δεδομένων, ανάγοντάς τα ως «αυτοτελές ατομικό δικαίωμα» και περιβάλλοντάς τα από ειδικές εγγυήσεις, προκειμένου να ελέγχονται οι σχετικές παραβάσεις. Η προστασία αυτή μέσω του Ν. 2472/1997 εφαρμόστηκε και στο εθνικό δίκαιο, με απώτερο σκοπό την εναρμόνιση της νομοθεσίας που ίσχυε στην Ελλάδα με τις ευρωπαϊκές επιταγές. Ο ανωτέρω νόμος συμπληρώθηκε και με τους υπ' αριθμ. 3471/2006, 3783/2009 και 3917/2011 Νόμους, όπως και με τις κανονιστικές πράξεις και Οδηγίες που εκδόθηκαν από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Η εφαρμογή του νόμου, σύμφωνα με την Οδηγία, εμπίπτει στην οιαδήποτε επεξεργασία δεδομένων ενός φυσικού προσώπου, οι οποίες περιλαμβάνονται σε αρχείο και εκτελούνται από τον υπεύθυνο επεξεργασίας ή από το άτομο που εκτελεί την επεξεργασία και ο οποίος εγκαθίσταται εντός της Ελλάδας ή τα μέσα επεξεργασίας, τα οποία χρησιμοποιεί είναι εγκατεστημένα στην Ελλάδα. Ωστόσο, η ισχύς του νόμου δεν καλύπτει την επεξεργασία των δεδομένων κατά τις προσωπικές ή οικιακές δραστηριότητες, ενώ εκτός της προστασίας είναι και η επεξεργασία των δεδομένων που πραγματοποιείται από τις Δημόσιες Αρχές, είτε αυτές είναι δικαστικές, είτε εισαγγελικές, είτε διοικητικές, με αποτέλεσμα τα προσωπικά δεδομένα των φυσικών προσώπων να καθίστανται σε πλήρη έκθεση.

2. Η ψήφιση του Κανονισμού 2016/679-GDPR για την προστασία των προσωπικών δεδομένων

Προχωρώντας, κρίνεται αναγκαίο να γίνουν αντιληπτοί μέσω βιβλιογραφικής ανασκόπησης, οι λόγοι που οδήγησαν στην ψήφιση του Κανονισμού. Με βάση την Ακριβοπούλου (2011), η νέα τεχνολογική πραγματικότητα δημιουργεί και διακινεί «επώνυμες» πληροφορίες, ήτοι «ευαίσθητα προσωπικά δεδομένα», ενισχύοντας με τον τρόπο αυτό την πιθανότητα να ελλοχεύει ο κίνδυνος να εκπέσουν οι πληροφορίες αυτές από τον έλεγχο των προσώπων που αφορούν. Η εξέλιξη αυτή δύναται να επιφέρει απώλεια της ιδιωτικής ζωής, με ότι αυτό συνεπάγεται για την ιδιοσυστασία του ανθρώπου και της προσωπικότητάς του, λόγω της υπερπροβολής και της μεγάλης έκθεσης που μπορεί να έχει υπάρξει. Μάλιστα, η δημιουργία «ψηφιδωτού» πληροφοριών έχει και τον κίνδυνο του να αλλοιωθούν και να μεταβληθούν οι πληροφορίες, καθώς και να χάσουν τον σκοπό για τον οποίο αυτές συλλέχθηκαν.

Σύμφωνα με τον Ιγγλεζάκη (2020), η διαρκής εξέλιξη της τεχνολογίας και η είσοδος στην εποχή της ψηφιοποίησης, σε συνδυασμό με την παγκοσμιοποίηση, ανέδυσαν νέες ανάγκες, οι οποίες δεν δύναται να καλυφθούν με την Οδηγία 95/46. Σημαντικός σταθμός στην επέλευση της αλλαγής αυτής υπήρξε η ταχύτατη εξέλιξη του διαδικτύου και των μέσων κοινωνικής δικτύωσης, καθώς μέσω της χρήσης αυτών αυξήθηκε και η επεξεργασία των μεγαδεδομένων (mega data), όπως και ο γεωεντοπισμός, η τεχνολογία RFID, η νεφοϋπολογιστική και άλλες επεμβατικές τεχνολογίες. Επιπλέον, η ανωτέρω ταχύτατη επέκταση των υπηρεσιών και χρηστών του διαδικτύου επέφερε και αύξηση στην επιτήρηση των υπηρεσιών τους, με αποτέλεσμα την επερχόμενη παραβίαση της προσωπικής ζωής των χρηστών και των προσωπικών δεδομένων τους.

Ως απόρροια των ανωτέρω, υπήρξε η ψήφιση στις 14 Απριλίου 2016 και η δημοσιοποίηση στην επίσημη Εφημερίδα της ΕΕ στις 04.05.2016 του Κανονισμού 2016/679. Ο Κανονισμός αυτός δεσμεύει όλα τα κράτη μέλη και ισχύει άμεσα σε αυτά σύμφωνα με το άρθρο 288 εδ. β' ΣΛΕΕ, εν αντιθέσει με την οδηγία, η οποία έχει εφαρμογή μόνο στα κράτη μέλη, στα οποία απευθύνεται. Συνεπώς, ο Κανονισμός δημιουργεί αποτελέσματα αμέσως στους πολίτες, επομένως και δικαιώματα υπέρ αυτών. Το γεγονός ότι ο Κανονισμός πρέπει να ενσωματώνεται στο δίκαιο που εφαρμόζει το κάθε κράτος μέλος και να μην έρχεται σε αντίθεση με

τον Κανονισμό, μέσω αντικρουόμενων νομοθετημάτων, καταδεικνύει την σημαντικότητα του και την υποχρεωτικότητα στην εφαρμογή του.

Σύμφωνα με τον Dove (2018), η ψήφιση του Κανονισμού θεωρήθηκε η σημαντικότερη πρωτοβουλία που θεσμοθετήθηκε σχετικά με την προστασία των προσωπικών δεδομένων. Τέθηκε στο επίκεντρο της ευρωπαϊκής νομοθεσίας και αποτέλεσε σημαντικό σταθμό για την ενίσχυση των εγγυήσεων της προστασίας των δικαιωμάτων των ατόμων. Ο GDPR εισήγαγε νέες απαιτήσεις, οι οποίες σχετίζονται με την υποχρεωτικότητα να διοριστεί εκπρόσωπος στην ΕΕ για τους υπευθύνους επεξεργασίας δεδομένων, και παράλληλα θέλησε να ενισχύσει την αρχή της διαφάνειας, θέτοντας ως υποχρεωτική την ενημέρωση του ατόμου σε περίπτωση παραβίασης των προσωπικών του δεδομένων.

Με βάση την Παναγοπούλου – Κουτνατζή (2018), ο Κανονισμός δημιουργήθηκε λόγω της ανάγκης για σύμπνοια του δικαίου με τις νέες τεχνολογίες, ενδυναμώνοντας συγχρόνως τα δικαιώματα των πολιτών. Ο Κανονισμός δηλώνει ρητά ότι η προστασία των προσωπικών δεδομένων δεν αποτελεί απόλυτο δικαίωμα, αλλά θα πρέπει να τίθεται σε στάθμιση και με άλλα δικαιώματα, τα οποία είτε αναγνωρίζονται στον Χάρτη, είτε περιλαμβάνονται στις Συνθήκες. Συνεπώς, η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής εξισορροπείται με την ανάγκη να απελευθερωθεί η κυκλοφορία των δεδομένων. Με την Οδηγία 95/46, και ιδίως με τον Ν. 2472/1997 υπήρχε η τάση για προτίμηση της προστασίας των προσωπικών δεδομένων έναντι της ελευθερίας της πληροφόρησης. Η «υπερπροστασία» αυτή δικαιολογείται λόγω του ενθουσιασμού που υπήρχε κατά την περίοδο που θεσπίστηκε ο Ν. 2472/1997. Μετά όμως από τον ενθουσιασμό ακολουθεί η ωρίμανση, η οποία δύναται να οδηγήσει στην ίδια διαχείριση των προσωπικών δεδομένων και στην υπό όρους ελεύθερη κυκλοφορία αυτών. Για το λόγο αυτό τα νέα ευρωπαϊκά νομοθετήματα, όπως και ο Κανονισμός, θέσπισαν ενιαίο πλαίσιο για την προστασία των δεδομένων και την ελευθερία της πληροφόρησης, με γνώμονα την αρχή της μη υπεροχής κανενός κατοχυρωμένου δικαιώματος, έναντι κάποιου άλλου.

Παράλληλα με τον Κανονισμό, εκδόθηκε και η Οδηγία 2016/680 που αφορά την προστασία των προσωπικών δεδομένων στις ποινικές υποθέσεις, υποχρεώνοντας τα κράτη-μέλη να την μεταφέρουν στο εθνικό τους δίκαιο. Ειδικότερα, η συγκεκριμένη «αστυνομική» Οδηγία στοχεύει στην εγκαθίδρυση κανόνων, οι οποίες σχετίζονται με την προστασία προσωπικών δεδομένων των φυσικών προσώπων έναντι της

επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές, ώστε να προληφθεί, διερευνηθεί, ανιχνευθεί ή διωχθεί κάθε ποινικό αδίκημα ή επιβληθεί ποινική κύρωση.

2.1. N. 4624/2019

Σύμφωνα με την αιτιολογική έκθεση του Ν. 4624/2019, όπως αυτή δημοσιεύθηκε μέσω της αρχής προστασίας των δεδομένων, ο Ν. 4624/2019 κατήργησε το προϊσχύσαν νομοθέτημα που ίσχυσε στην Ελλάδα, ήτοι το Ν. 2472/1997, και θέσπισε μέτρα, τα οποία σχετίζονται με τον Κανονισμό 2016/679, ενσωματώνοντας συγχρόνως στο εθνικό δίκαιο την Οδηγία 2016/680. Ο νόμος σκοπεύει να αντικαταστήσει το υπάρχον πλαίσιο και να προβεί στην θέσπιση κανόνων, οι οποίες συμβαδίζουν με τον Κανονισμό. Σε αντίθεση με το προηγούμενα νομοθετήματα, ο νόμος αυτός έχει εφαρμογή κατά την αυτοματοποιημένη ή μη επεξεργασία δεδομένων, τα οποία πρόκειται να αρχειοθετηθούν τόσο από δημόσιους φορείς, όσο και από ιδιωτικούς.

Ως «δημόσιοι φορείς» νοούνται οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού, τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκηση τους ορίζεται από αυτό.

Με βάση τον Ιγγλεζάκη (2020), σχετικά με τους ιδιώτες, ο νόμος έχει εφαρμογή υπό συγκεκριμένες προϋποθέσεις. Ειδικότερα, εφαρμόζεται στις περιπτώσεις που οι ιδιώτες θέτουν σε επεξεργασία προσωπικά δεδομένα, συμπεριλαμβάνοντας και τους ελεύθερους επαγγελματίες, όπως είναι οι δικηγόροι, γιατροί, λογιστές κλπ. Από την ανωτέρω εφαρμογή εξαιρούνται τα πρόσωπα που επεξεργάζονται δεδομένα υπό καθεστώς προσωπικών ή οικιακών δραστηριοτήτων, όπως το να τηρούνται αρχεία διευθύνσεων έντυπης ή ηλεκτρονικής αλληλογραφίας ή το να λαμβάνονται ιδιωτικές φωτογραφίες, καθώς επίσης και τα δεδομένα σε παιχνιδομηχανές ή τα συστήματα smart-home, αλλά και οι προσωπικές σελίδες στα μέσα κοινωνικής δικτύωσης ή η επεξεργασία δεδομένων που πραγματοποιείται για προσωπικούς λόγους, όπως είναι το χόμπι ή μια δραστηριότητα.

Περαιτέρω, με βάση τον Χριστοδούλου (2020), γίνεται αντιληπτό ότι και το δίκαιο για την προστασία των προσωπικών δεδομένων έχει υπόβαθρο πολιτικό, συγκρούοντας τις ιδεολογικές πεποιθήσεις του φιλελευθερισμού και του σοσιαλισμού. Ειδικότερα, δημιουργείται ένα φράγμα που εμποδίζει την ελεύθερη κυκλοφορία των πληροφοριών, διασφαλίζοντας συγχρόνως την ιδιωτική αυτονομία και την ελεύθερη αυτοδιάθεση του ατόμου.

2.2. Όργανα για την προστασία των προσωπικών δεδομένων

Στο σημείο αυτό, κρίνεται απαραίτητη να γίνει η βιβλιογραφική ανασκόπηση σχετικά με τα όργανα που παίζουν βασικό ρόλο στην προστασία των προσωπικών δεδομένων. Σύμφωνα με τον Ιγγλεζάκη (2020), με τον Κανονισμό Προστασίας Δεδομένων καθιερώθηκε ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ). Ειδικότερα, υποχρεώθηκαν οι υπεύθυνοι επεξεργασίας και εκτελούντες αυτής στην οργάνωση ενός εσωτερικού συστήματος ελέγχου, μέσω του οποίου θα συμμορφώνονται οι ανωτέρω με τις διατάξεις που προβλέπει ο Κανονισμός. Επομένως, επιβλήθηκε εμμέσως η ισχύς της αρχής της λογοδοσίας, καθώς μέσω του ΥΠΔ παρακολουθούνταν η συμμόρφωση με τις επιταγές του ΓΚΠΔ.

Σύμφωνα με τον Κανονισμό, ως υπεύθυνος προστασίας δεδομένων νοείται το πρόσωπο που επιβαρύνεται με το γνωστικό στοιχείο της προστασίας των προσωπικών δεδομένων. Διαθέτει, δηλαδή, εξειδικευμένες γνώσεις, οι οποίες δύναται να ενισχύσουν την προσπάθεια του να παρακολουθεί την εσωτερική συμμόρφωση των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία με τον ΓΚΠΔ. Ο ΥΠΔ δύναται να είναι εσωτερικός ή εξωτερικός. Επομένως, μπορεί να βρίσκεται υπό το πέπλο της σύμβασης εργασίας με τον υπεύθυνο επεξεργασίας δεδομένων ή να διαθέτει μόνο συμβουλευτικό ρόλο. Ωστόσο, θα πρέπει να εμποτίζεται με προσόντα και ικανότητες, οι οποίες να συμβάλλουν στην επίτευξη του σκοπού, για τον οποίο ορίζεται. Πρέπει δε να υπογραμμιστεί ότι αποτελεί ανεξάρτητο όργανο, ο οποίος ακόμη και στην περίπτωση της ύπαρξης σχέσης εξαρτημένης εργασίας, διατηρεί την αυτονομία του.

Επιπλέον, υφίσταται και ο υπεύθυνος επεξεργασίας, ο οποίος είναι διαφορετικός από τον υπεύθυνο προστασίας δεδομένων, παρά την σύγχυση που δημιουργείται. Ο υπεύθυνος επεξεργασίας ευθύνεται για την τήρηση των υποχρεώσεων και διαδικασιών και για την ανταπόκριση στα αιτήματα που σχετίζονται με τα

δικαιώματα του υποκειμένου των δεδομένων. Θεωρείται ιδιαίτερα κρίσιμο το ποιος θα καθοριστεί ως υπεύθυνος επεξεργασίας, καθώς σχετίζεται με την λειτουργία του ΥΠΔ, αφού ο ΥΠΔ ορίζεται είτε από τον υπεύθυνο επεξεργασίας, είτε από τον εκτελούντα την επεξεργασία.

Σε ορισμένες περιπτώσεις είναι πιθανή η συνύπαρξη πολλαπλών υπευθύνων επεξεργασίας ή συνυπευθύνων επεξεργασίας, προκειμένου ο καθένας να αναλάβει μια διαφορετική πτυχή της επεξεργασίας. Η εξακρίβωση για το εάν ένα πρόσωπο έχει το ρόλο του υπευθύνου επεξεργασίας γίνεται με την αποτύπωση των λόγων μέσω των οποίων δικαιολογείται η επεξεργασία, δηλαδή των μέσων και των σκοπών. Επίσης, κρίνεται και από τον τρόπο που το όργανο ή το πρόσωπο ελέγχει τις μεθόδους επεξεργασίας, τα δεδομένα που πρόκειται να υποβληθούν προς επεξεργασία, καθώς και από τα άτομα που επεξεργάζονται τα δεδομένα αυτά.

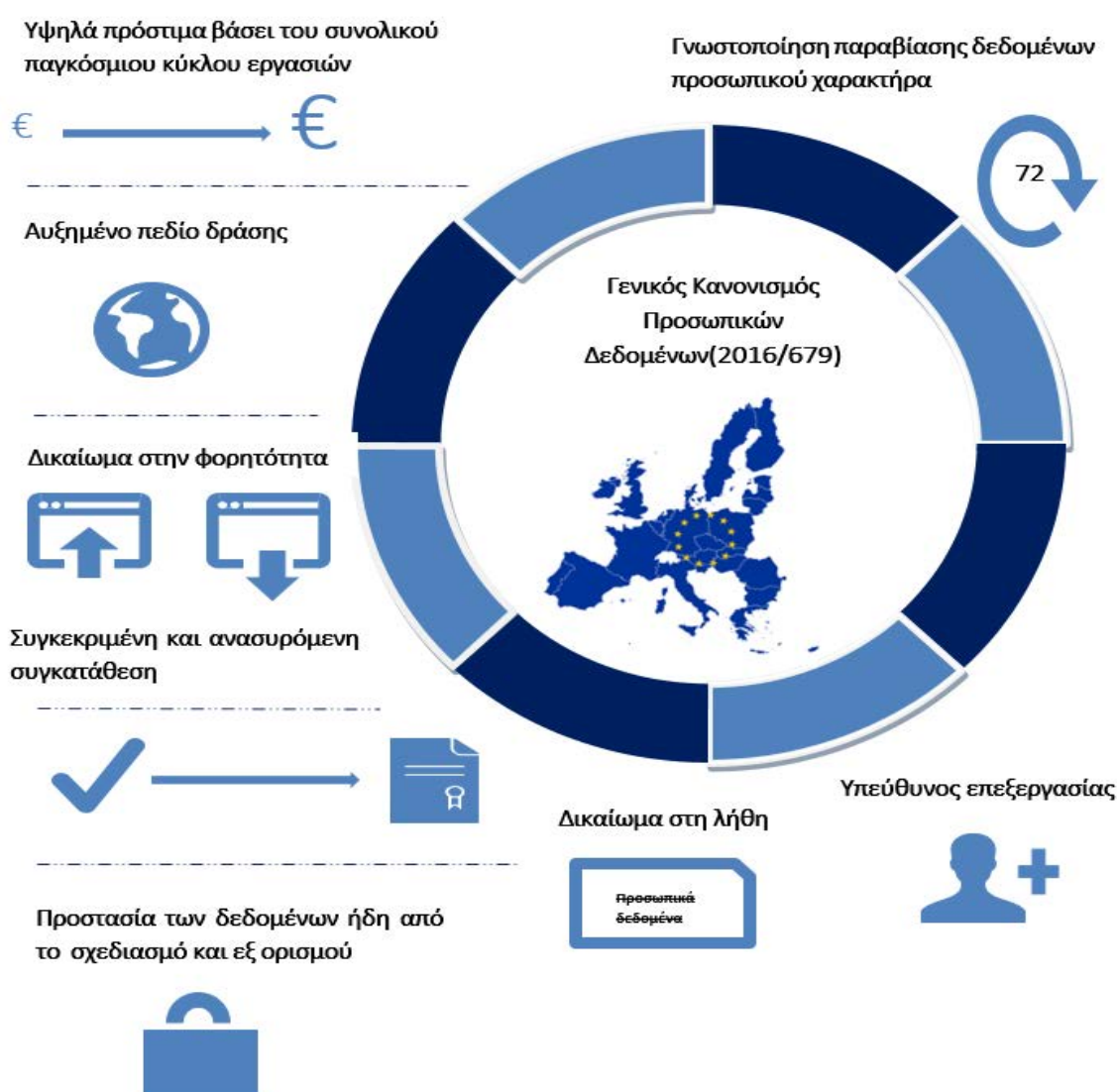
Τα πρόσωπα, τα οποία εκπίπτουν του υπευθύνου επεξεργασίας και επεξεργάζονται οι ίδιοι τα δεδομένα, αντί του υπευθύνου επεξεργασίας θεωρούνται εκτελούντες την επεξεργασία. Ωστόσο και σε αυτή την περίπτωση η ευθύνη βαρύνει τον υπεύθυνο επεξεργασίας.

Ο εκτελών την επεξεργασία είναι διαφορετικός από τον υπεύθυνο επεξεργασίας. Ειδικότερα, ο εκτελών είναι φυσικό ή νομικό πρόσωπο, το οποίο εκφεύγει της εποπτείας του υπευθύνου επεξεργασίας και επεξεργάζεται δεδομένα «για λογαριασμό» του υπευθύνου επεξεργασίας. Η σημαντικότερη διαφορά ανάμεσα στα δύο ανωτέρω πρόσωπα, είναι ότι ο εκτελών την επεξεργασία δεν αναλαμβάνει τον καθορισμό του σκοπού και του τρόπου της επεξεργασίας, αλλά αυτό πραγματοποιείται από τον υπεύθυνο επεξεργασίας. Αντιθέτως ο ρόλος του εκτελούντος την επεξεργασία προσώπου είναι η ανάληψη της διεξαγωγής της επεξεργασίας των δεδομένων, κατόπιν εντολών που δίνονταν από τον υπεύθυνο επεξεργασίας. Σύμφωνα με τα ανωτέρω η αναφορά στον Κανονισμό της φράσης «για λογαριασμό», σημαίνει ότι η επεξεργασία γίνεται υπό τις οδηγίες του υπευθύνου επεξεργασίας. Αν ο εκτελών την επεξεργασία, εκφύγει αυτών των οδηγιών και ενεργήσει αυτοβούλως, τότε θεωρείται ο ίδιος υπεύθυνος επεξεργασίας, αφού έχει καθορίσει και διαμορφώσει τον τρόπο που θα επιτευχθεί η επεξεργασία των δεδομένων.

Επιπλέον, με βάση τον Σωτηρόπουλο (2019), τα πρόσωπα που παίζουν επίσης σημαντικό ρόλο στην επεξεργασία των δεδομένων είναι ο «τρίτος» και ο «αποδέκτης». Ως τρίτος θεωρείται το πρόσωπο που απασχολείται σε έναν φορέα, ο οποίος διαφοροποιείται από αυτόν του υπευθύνου επεξεργασίας και του εκτελούντα την

επεξεργασία, ακόμη και αν περιλαμβάνονται στον ίδιο όμιλο ή στην ίδια μητρική εταιρεία. Αντιθέτως, δεν θεωρούνται τρίτοι τα καταστήματα μιας τράπεζας, τα οποία θέτουν σε επεξεργασία λογαριασμούς πελατών, οι οποίοι εποπτεύονται από την κεντρική διοίκηση.

Τέλος, ως αποδέκτης νοείται το πρόσωπο, το οποίο είναι εκτός του υπευθύνου επεξεργασίας ή του προσώπου που εκτελεί την επεξεργασία ή κάποιος εσωτερικός που συνεπικουρεί τον ρόλο του υπευθύνου επεξεργασίας ή του εκτελούντα. Ο αποδέκτης γίνεται λήπτης δεδομένων και είναι στην διακριτική του ευχέρεια, αν θα προβεί στην διατήρηση ή στην απόρριψη αυτών.



Εικόνα 2.2.1. Γενικός Κανονισμός Προσωπικών Δεδομένων (2016/679)

3. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων στις επιχειρήσεις

Προχωρώντας, κρίνεται αναγκαίο να γίνει βιβλιογραφική ανασκόπηση, για τα GDPR στις επιχειρήσεις. Με βάση την Europa (2014), ο Γενικός Κανονισμός για την Προστασία των Δεδομένων, γνωστός και ως General Data Protection Regulation (GDPR), αλλάζει ριζικά τον τρόπο με τον οποίο επιχειρήσεις και οργανισμοί συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα κάθε μορφής. Ο GDPR καθορίζει σε ποιες περιπτώσεις επιτρέπεται να χρησιμοποιούνται, αποθηκεύονται, διαγράφονται, μεταβιβάζονται και εν γένει επεξεργάζονται τα προσωπικά μας δεδομένα και κυρίως, με ποιον τρόπο μπορούμε να τα προστατεύουμε. Ο GDPR επηρεάζει κάθε οργανισμό και εταιρεία στην Ευρώπη, η οποία διαχειρίζεται με οποιονδήποτε τρόπο προσωπικά δεδομένα, αλλά και κάθε εταιρεία που συναλλάσσεται στην επικράτεια της Ευρωπαϊκής Ένωσης. Οι κανόνες είναι πολύπλοκοι και τα πρόστιμα για μη συμμόρφωση πολύ αυστηρά και μπορούν να φτάσουν έως τα 20 εκατομμύρια ευρώ.

Σύμφωνα με τον Tikkinen-Piri (2018), ο GDPR επηρεάζει τα μέτρα που πρέπει να λαμβάνονται σχετικά με την προστασία της ιδιωτικής ζωής. Ειδικότερα, εμπεριέχει σημαντικά μέτρα για την προστασία της ιδιωτικής ζωής, που σχετίζονται τόσο με το οργανωτικό μέρος, όσο και με το τεχνικό. Ωστόσο, για την εφαρμογή των μέτρων από τους οργανισμούς και τις επιχειρήσεις, απαιτείται χρόνος, προγραμματισμός, ειδική εκπαίδευση και πόροι. Ως πρωταρχικός στόχος των GDPR αποτελεί η ενίσχυση της εμπιστοσύνης των ατόμων απέναντι στους φορείς που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα, ενώ παράλληλα στοχεύει και στην παροχή ωφέλειας στις εταιρείες, βοηθώντας τις στην εφαρμογή του απορρήτου των δεδομένων και στις ειδικές πτυχές που πρέπει να ληφθούν υπόψιν.

Με βάση την Παναγοπούλου-Κουτνατζή (2018), σύμφωνα με τον Κανονισμό, *«το δικαίωμα της προστασίας προσωπικών δεδομένων δεν αποτελεί απόλυτο δικαίωμα»*. Συνεπώς, θα πρέπει να αντισταθμίζεται η προστασία του, με την προστασία και άλλων θεμελιωδών δικαιωμάτων, σύμφωνα και με την αρχή της αναλογικότητας. Ειδικότερα, ο Κανονισμός προασπίζει όλα τα δικαιώματα που αναφέρονται στο Χάρτη Θεμελιωδών Δικαιωμάτων, όπως αποτελεί ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, της προστασίας δεδομένων προσωπικού χαρακτήρα, της ελευθερίας σκέψης,

συνείδησης και θρησκείας, της ελευθερίας έκφρασης και πληροφόρησης, της επιχειρηματικής ελευθερίας, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία.

Με βάση τον Ιγγλεζάκη (2018), ο Κανονισμός εφαρμόζεται κατά την επεξεργασία των προσωπικών δεδομένων των υποκειμένων από υπεύθυνο επεξεργασίας, τα οποία βρίσκονται εντός της Ευρωπαϊκής Ένωσης και σχετίζονται με δραστηριότητες που αφορούν είτε προσφορά αγαθών ή υπηρεσιών, ανεξάρτητα αν απαιτείται πληρωμή ή όχι από τα υποκείμενα των δεδομένων, είτε την παρακολούθηση της συμπεριφοράς τους.

Ως σκοπός του Κανονισμού Προστασίας Δεδομένων αποτελεί η διαχείριση των προσωπικών δεδομένων να πραγματοποιείται με ασφαλή τρόπο τόσο από τους φορείς όσο και από τις επιχειρήσεις που δραστηριοποιούνται στον ιδιωτικό και στον δημόσιο τομέα. Η θέσπιση, δηλαδή, ενιαίων κανόνων συμβάλει στην προστασία των φυσικών προσώπων από την επεξεργασία προσωπικών δεδομένων, με παράλληλη προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και συγκεκριμένα της προστασίας των δεδομένων.

Σύμφωνα με τα στοιχεία της Europa (2022), ο Κανονισμός διαμορφώνει τις προϋποθέσεις, σύμφωνα με τις οποίες η εκάστοτε επιχείρηση θα δύναται να δραστηριοποιείται εντός της Ευρωπαϊκής Ένωσης με ισότιμους όρους, διαμορφώνοντας τις συνθήκες για καινοτομία. Ειδικότερα, πλέον υφίσταται ενιαίο νομοθετικό πλαίσιο στην εσωτερική αγορά της ΕΕ, δημιουργώντας μεγαλύτερη ασφάλεια δικαίου. Προστίθεται ο υπεύθυνος προστασίας δεδομένων, ο οποίος ορίζεται από τις δημόσιες αρχές είτε από τις επιχειρήσεις, οι οποίες θέτουν σε επεξεργασία δεδομένα με μεγάλη συχνότητα ή τα δεδομένα αυτά αφορούν ειδικές κατηγορίες. Επιπλέον, τίθενται σε εφαρμογή η υπηρεσία μίας στάσης, δηλαδή η εποπτική αρχή στην οποία υπάγεται πλέον η εκάστοτε επιχείρηση. Ακόμη, προκειμένου να επιτευχθεί η καινοτομία, ο Κανονισμός περιλαμβάνει τις εγγυήσεις για την προστασία των δεδομένων που σχετίζεται με τα προϊόντα και τις υπηρεσίες, οι οποίες προστατεύονται ήδη από το πρώιμο στάδιο ανάπτυξης του. Επίσης, γίνεται προτροπή στις επιχειρήσεις να χρησιμοποιούν τεχνικές, οι οποίες είναι φιλικές με την προστασία της ιδιωτικής ζωής, όπως αποτελεί η ψευδωνυμοποίηση και η κρυπτογράφηση, ώστε να γίνεται περιορισμός της επεξεργασίας των δεδομένων, με την χρήση δηλαδή τεχνητών αναγνωριστικών ή κωδικοποιημένων δεδομένων.

Με βάση τον Ιγγλεζάκη (2020), στον τομέα των επιχειρήσεων, η ύπαρξη του ΥΠΔ προσφέρει ανταγωνιστικό πλεονέκτημα στην εκάστοτε επιχείρηση, αφού συνεπικουρεί στο έργο των υπευθύνων επεξεργασίας ή εκτελούντων αυτής, προκειμένου να συμμορφώνονται με τον Κανονισμό. Σε περίπτωση δε που η επιχείρηση δεν συμμορφώνεται με τον Κανονισμό, η ευθύνη βαρύνει μόνο τον υπεύθυνο επεξεργασίας και όχι τον ΥΠΔ. Η ανάγκη ύπαρξης του ΥΠΔ σε μία επιχείρηση αναδύεται από την φύση των δραστηριοτήτων της και του μεγέθους των δεδομένων που αυτή επεξεργάζεται.

Η υποχρεωτικότητα στον ορισμό του ΥΠΔ γεννάται στις περιπτώσεις των επιχειρήσεων, οι οποίες προβαίνουν κατά βάση σε τακτική και συστηματική παρακολούθηση σε μεγάλο εύρος, η οποία ενισχύεται και μέσω του Διαδικτύου. Τέτοια επιχείρηση μπορεί να θεωρηθεί η Τράπεζα, η οποία επεξεργάζεται τα δεδομένα των πελατών της προκειμένου να προβαίνει σε συμπεριφορική διαφήμιση. Η μεγάλη επιρροή των δεδομένων αυξάνει και την πιθανότητα εκδήλωσης κινδύνου κατά την επεξεργασία.

Ως βασικοί παράγοντες, οι οποίοι πρέπει να λαμβάνονται υπόψιν είναι το πλήθος των εμπλεκόμενων προσώπων, τα οποία καθίστανται υποκείμενα επεξεργασίας δεδομένων, η ποσότητα των δεδομένων, τα οποία τίθενται προς επεξεργασία, η διάρκεια χρήσης των δεδομένων, η οποία έρχεται σε συνάφεια με την δραστηριότητα της επιχείρησης και η γεωγραφική έκταση της.

Στις περιπτώσεις ύπαρξης ομίλου επιχειρήσεων, σύμφωνα με το άρθρ. 37 παρ. 2 ΓΚΠΔ, δύναται να διοριστεί και ένας μόνο ΥΠΔ, εφόσον όμως είναι εφικτή η συνεργασία και επικοινωνία με τον υπεύθυνο προστασίας δεδομένων και τις αρμόδιες αρχές. Για το λόγο αυτό είναι απαραίτητο να τίθενται δημόσια τα στοιχεία του ΥΠΔ, ώστε να διευκολύνεται η επικοινωνία.

3.1. Τα GDPR στις μικρές και μικρομεσαίες επιχειρήσεις

Στο σημείο αυτό, θα γίνει περαιτέρω εμβάθυνση με την βοήθεια της βιβλιογραφίας, προκειμένου να αναδειχθεί η σημασία των GDPR στις μικρομεσαίες επιχειρήσεις. Με βάση τα στοιχεία που συλλέχθηκαν από την Αρχή Προστασίας Δεδομένων, οι μικρές και οι μικρομεσαίες επιχειρήσεις είναι απαραίτητο να δίνουν προσοχή σε ορισμένα σημεία κατά την δραστηριοποίηση τους. Σήμερα, η πλειοψηφία των δραστηριοτήτων των μικρών και μεσαίων επιχειρήσεων πραγματοποιείται ηλεκτρονικά ή μέσω του διαδικτύου. Ωστόσο, οι περισσότερες επιχειρήσεις, οι οποίες είναι μικρές αλλά και οι μεσαίες, δεν δίνουν την απαραίτητη προσοχή στην ηλεκτρονική τους παρουσία και στις ηλεκτρονικές εφαρμογές τους, με αποτέλεσμα να παρουσιάζονται περιστατικά παραβίασης, τα οποία γίνονται γνωστά στις εποπτικές αρχές. Για λόγους λοιπόν οικονομίας κυρίως χρημάτων αλλά και χρόνου, παραλείπουν το βασικό στάδιο που αφορά την παρουσία της επιχείρησης στον διαδικτυακό ιστότοπο, αλλά και την εκπαίδευση του προσωπικού με αποτέλεσμα να έρχονται στην συνέχεια αντιμέτωποι με παραβιάσεις προσωπικών δεδομένων, στις οποίες οι ίδιες οι επιχειρήσεις έχουν υποπέσει.

Χαρακτηριστικά παραδείγματα αποτελούν οι αποστολές μηνυμάτων ηλεκτρονικού ταχυδρομείου (email), οι οποίες περιέχουν δεδομένα προσωπικού χαρακτήρα σε λανθασμένο σύνολο αποδεκτών. Επίσης, έντονο είναι το φαινόμενο του εξωτερικού κακόβουλου χρήστη, ο οποίος υπεισέρχεται σε κωδικούς χρηστών ή εκμεταλλεύεται την μη εγκατάσταση τελευταίας ενημερωμένης έκδοσης. Επιπρόσθετα, συχνά γίνεται διαρροή πληροφοριών από επιχειρήσεις και καθίστανται αυτές δημοσίως προσβάσιμες, ενώ αναγράφονται σε ιστοσελίδες, όχι όμως για δημόσια προβολή. Πρόβλημα, επίσης, δημιουργείται με τους φορητούς ηλεκτρονικούς υπολογιστές και τα αποθηκευτικά μέσα, τα οποία δύνανται να χαθούν ή να κλαπούν.

Σύμφωνα με τον Wheatley (2016), όλο και αυξάνονται τα περιστατικά των παραβιάσεων στην συλλογή και επεξεργασία των δεδομένων. Μάλιστα, το πόσο συχνά και πόσο σοβαρή είναι η μορφή της παραβίασης εξαρτάται από το πόσο μεγάλοι είναι οι οργανισμοί και οι επιχειρήσεις και πόσο εκτεθειμένοι είναι στον κίνδυνο της παραβίασης. Αναφορές δε επιβεβαιώνουν τα ανωτέρω και καταλήγουν στο συμπέρασμα ότι αναμένεται συνεχή αύξηση των παραβιάσεων. Οι παραβιάσεις δε αυτές επίκειται να δημιουργήσουν αρνητικές επιπτώσεις, με αποκορύφωμα την

οικονομική καταστροφή των ιδίων των προσώπων, των οποίων τίθενται προς επεξεργασία τα δεδομένα ή και των επιχειρήσεων, οι οποίες επεξεργάζονται τα προσωπικά δεδομένα, ειδικά όταν συναντώνται φαινόμενα μαζική εξαπάτησης.

Με βάση τον Algarni (2021), όταν οι παραβιάσεις των δεδομένων έχουν οικονομικό αντίκτυπο, αυτό δύναται να επηρεάσει τόσο τους οργανισμούς, όσο και γενικά την οικονομία παγκοσμίως. Ειδικότερα, απαιτείται αυξημένο κόστος, προκειμένου να εντοπιστεί αρχικά από που προήλθε η παραβίαση και στην συνέχεια για την αντιμετώπιση αυτής της παραβίασης. Πέρα όμως, από τα άμεσα και εξόφθαλμα κόστη, υπάρχουν και τα έμμεσα κόστη, τα οποία δημιουργούν περαιτέρω προβλήματα στις ίδιες επιχειρήσεις. Αυτά σχετίζονται με την φήμη, αλλά και γενικώς την απώλεια της εμπιστοσύνης των ατόμων έναντι των επιχειρήσεων.

Η πολύ πρόσφατη δημοσίευση των Aldboush & Ferdous (2023), ανέφερε ότι η εμπιστοσύνη είναι ένας βασικός παράγοντας που επηρεάζει την προσέλκυση και διατήρηση των πελατών στις επιχειρήσεις. Αν υπάρχει κρίση και απώλεια της εμπιστοσύνης, θα μειωθεί και η αφοσίωση αυτών με αποτέλεσμα οι καταναλωτές να αρχίζουν να απομακρύνονται. Αυτό φυσικά θα έχει ως περαιτέρω αποτέλεσμα να απωλεσθούν σημαντικά ποσά εσόδων και κερδών για τις επιχειρήσεις.

Σύμφωνα με την Αρχή Προστασίας Δεδομένων, για την αποτροπή των ανωτέρω, οι επιχειρήσεις συνίσταται να προβαίνουν καταρχάς σε κατάλληλη ενημέρωση των χρηστών, με την εισαγωγή διαδικασιών που ελέγχουν και επιβεβαιώνουν τα email των παραληπτών. Επιπλέον, κρίνεται σημαντικό να πραγματοποιείται κρυπτογράφηση από τις επιχειρήσεις κατά την αποστολή των αρχείων που περιέχουν προσωπικά δεδομένα τα οποία ανήκουν σε ειδικές κατηγορίες ή πρόκειται να έχουν σημαντικές συνέπειες για τα υποκείμενα των δεδομένων που αφορούν. Λύση σε αυτό είναι η αποστολή ή παράδοση στην πρώτη επαφή ή στο στάδιο που πραγματοποιείται η πρώτη επικοινωνία, ενός «κλειδιού» για να δίνει πρόσβαση στην κρυπτογράφηση. Επιπροσθέτως, οι επιχειρήσεις πρέπει να μπαίνουν σε διαδικασία ενημέρωσης και ευαισθητοποίησης των χρηστών, είτε μέσω σχετικών δράσεων, είτε με δικές τους παρεμβάσεις και ενημερώσεις, ώστε να είναι σε θέση να αποτρέπουν τους ανωτέρω κινδύνους και να κατανοούν το νόημα τόσο της επιλογής ισχυρών κωδικών κατά την χρήση, όσο και της εγκατάστασης εφαρμογών, οι οποίες περιέχουν ενημερώσεις ασφάλειας. Με τον τρόπο αυτό θα υπάρχει πολυπλοκότητα στους χαρακτήρες, δυσκολεύοντας το έργο των «hacker» και θα μειώνεται η πιθανότητα να βρίσκονται τα προσωπικά τους δεδομένα εκτεθειμένα σε

κακόβουλους χρήστες. Είναι αναγκαίο να υπογραμμιστεί ότι οι περισσότερες περιπτώσεις παραβιάσεων προσωπικών δεδομένων είναι απόρροια ανθρώπινου λάθους. Είτε δηλαδή ευθύνεται η ίδια η επιχείρηση και το προσωπικό της, είτε και οι χρήστες, οι οποίες είναι ελλιπώς ενημερωμένοι και ευάλωτοι.

Στα τέλη Απριλίου 2023, ανακοινώθηκε η δημιουργία του Οδηγού Προστασίας Δεδομένων για μικρές επιχειρήσεις από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, στο οποίο είχε συμμετοχή και η ελληνική αρχή, ο οποίος αρχικά ήταν διαθέσιμος μόνο στα αγγλικά και στις 24 Ιουλίου 2024 έγινε η έκδοση του και στα ελληνικά. Ο ανωτέρω Οδηγός αποτελεί ένα επιβοηθητικό εργαλείο για την κάθε μικρή και μικρομεσαία επιχείρηση, ο οποίος θα ενισχύσει την προσπάθεια τους για συμμόρφωση με τον ΓΚΠΔ.

Πρωτίστως, είναι σημαντικό η εκάστοτε επιχείρηση να αντιληφθεί τι εστί προσωπικά δεδομένα. Ειδικότερα, κρίνεται αναγκαίο να γίνει αντιληπτό πως οποιοδήποτε στοιχείο ταυτοποιεί άμεσα ή έμμεσα ένα πρόσωπο, θεωρείται προσωπικό δεδομένο. Αυτό μπορεί να είναι όνομα, επίθετο, αριθμός τηλεφώνου ενός πελάτη, εργαζομένου ή ενδιαφερόμενου μέρους, αλλά και ένας αριθμός κράτησης ή αναγνώρισης αυτού, η διεύθυνση ηλεκτρονικού ταχυδρομείου, το ιστορικό περιήγησης, όπως και βίντεο, φωτογραφίες και ηχογραφήσεις.

Εκτός των ανωτέρω, υφίστανται και ειδικές κατηγορίες προσωπικών δεδομένων, οι οποίες καλούνται «ευαίσθητες» και εμπεριέχουν πληροφορίες που σχετίζονται με την υγεία του ατόμου, τον σεξουαλικό ή γενετήσιο προσανατολισμό του, τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τα βιομετρικά και γενετικά δεδομένα ενός ατόμου και την συμμετοχή του σε συνδικαλιστικές οργανώσεις. Η επεξεργασία αυτού του είδους των δεδομένων γίνεται υπό συγκεκριμένες προϋποθέσεις και κυρίως όταν υπάρχει ρητή συγκατάθεση του ατόμου, ειδάλλως απαγορεύεται.

Επιπλέον, τα προσωπικά δεδομένα ενός ατόμου, που σχετίζονται με ποινικές καταδίκες και αδικήματα επεξεργάζονται μόνο υπό αυστηρούς όρους και κυρίως από επίσημες αρχές, εφόσον γίνεται επιτρεπτό από το δίκαιο.

Κάθε επιχείρηση ή οργανισμός είναι εφικτό να επεξεργάζεται προσωπικά δεδομένα υπό το πέπλο της νομιμότητας, αντικειμενικότητας και διαφάνειας. Για να θεωρείται νόμιμη, πρέπει να εδράζεται στην συγκατάθεση του ατόμου, η οποία είναι απαραίτητη όταν εκτελείται μια σύμβαση. Η συγκατάθεση πρέπει να προσφέρεται ελεύθερα, έχοντας πλήρη επίγνωση των δυνατοτήτων που δίνονται με αυτή, ήτοι την

επεξεργασία που μπορεί να ακολουθήσει από τους οργανισμούς. Επιπροσθέτως, τα άτομα πρέπει να έχουν την δυνατότητα σε περίπτωση που αλλάζουν γνώμη, να δύναται να προβούν σε ανάκληση της συγκατάθεσης. Είναι δε αναγκαίο οι επιχειρήσεις να συλλέγουν μόνο τα προσωπικά δεδομένα που εξυπηρετούν συγκεκριμένους, προκαθορισμένους και νόμιμους σκοπούς, χωρίς αυτοί να μεταβάλλονται στην πορεία και να μην συμβαδίζουν με τους αρχικούς.

3.2. Τα GDPR και η εφαρμογή τους από τα πιστωτικά ιδρύματα

Σύμφωνα με τον Ρόκα κλπ (2016), ανάμεσα στον πελάτη και τα πιστωτικά ιδρύματα αναπτύσσεται μια σχέση, η οποία βασίζεται στην καλή πίστη και στα συναλλακτικά ήθη, καθώς και στην εμπιστοσύνη και την εχεμύθεια. Οι τράπεζες, ως το ισχυρότερο μέρος εκ των δύο συμβαλλομένων, πρέπει να προστατεύουν τους καταναλωτές. Αυτό έχει ως απόρροια ήδη από το 1997, η Ελληνική Ένωση Τραπεζών να προέβη στην δημιουργία κωδίκων δεοντολογίας, οι οποίοι ακολουθούν και δεσμεύουν τα πιστωτικά ιδρύματα σε κάθε τους βήμα και αποτελούν τρόπο έκφρασης της «αυτορρύθμισης» τους. Οι κανόνες που εμπεριέχονται στους κώδικες δεν αποτελούν αναγκαστικού δικαίου, αλλά έχουν ήπιο χαρακτήρα (soft law). Για το λόγο αυτό πολλές φορές η εφαρμογή της δεν είναι δυνατή.

Συνεπώς, «αναγκάζονται» από τις συνθήκες να τροποποιηθούν ή να μετεξελιχθούν σε νομοθετικό κείμενο, του οποίου η εφαρμογή δε μπορεί να είναι απροσπέλαστη. Αθέμιτες πρακτικές των Τραπεζών, οι οποίες δε συνάδουν με τους κώδικες δεοντολογίας, δεν γίνονται αποδεκτές από το κανονιστικό πλαίσιο, το οποίο εμπεριέχει συγκεκριμένα μοτίβα συμπεριφοράς, που επιτρέπονται από τις Τράπεζες.

Ως απόρροια των ανωτέρω ήταν η εκπόνηση του Κώδικα Δεοντολογίας για την επεξεργασία προσωπικών δεδομένων στο τραπεζικό σύστημα από την Ελληνική Ένωση Τραπεζών, σύμφωνα με τον οποίο συνεργάστηκαν τα μέλη-τράπεζες της ένωσης, ώστε να προβούν στην εφαρμογή του άρθρου 40 του ΓΚΠΔ. Ο Κανονισμός, δηλαδή, παροτρύνει την δημιουργία ενός κώδικα με βάση τον οποίο θα μπορούν να συμπλέουν τα πιστωτικά ιδρύματα, για να προστατεύουν τα προσωπικά δεδομένα και να προωθούν την ελεύθερη κυκλοφορία τους. Μέσω του Κώδικα Δεοντολογίας τίθενται οι βασικές αρχές, οι οποίες αποτελούν την βάση της επεξεργασίας των δεδομένων και ισχυροποιούν την ασφάλεια δικαίου, συμβάλλοντας στην ενίσχυση των σχέσεων του πελατών με τα πιστωτικά ιδρύματα.

Με βάση την Τράπεζα της Ελλάδος, τίθενται προς επεξεργασία δεδομένα προσωπικού χαρακτήρα, τα οποία είναι αναγκαία για την υλοποίηση των λειτουργιών της, χωρίς να κοινοποιούνται σε τρίτους για εμπορικούς σκοπούς. Μάλιστα, η επεξεργασία αυτή γίνεται με γνώμονα τις αρχές του Γενικού Κανονισμού για την Προστασία Δεδομένων. Αρμόδιος ως υπεύθυνος για την επεξεργασία δεδομένων είναι η Τράπεζα της Ελλάδος και μόνο μέλη του προσωπικού της θα δύναται να προβαίνουν σε επεξεργασία των δεδομένων που χρειάζονται. Αυτά, όμως, τα δεδομένα προσωπικού χαρακτήρα δεν δύνανται να κοινοποιηθούν σε τρίτους, χωρίς να συγκαταθέσουν και τα ίδια τα πρόσωπα, τα οποία αφορά. Η Τράπεζα, επίσης, χρησιμοποιεί τα «cookies», δηλαδή πολύ μικρά αρχεία κειμένου πληροφορίας, κατά την χρήση από τους browsers (Chrome, Mozilla Firefox κ.λπ.), οι οποίες πρόκειται να βελτιώσουν την εμπειρία των χρηστών κατά την περιήγηση τους στον διαδικτυακό ιστότοπο. Η χρήση των cookies από την Τράπεζα πραγματοποιείται μόνο για τις απαιτούμενες λειτουργίες, χωρίς να επιτρέπεται η συγκέντρωση πληροφοριών που αφορούν τους επισκέπτες και η προώθηση αυτών. Δίνεται, βέβαια και η επιλογή στους χρήστες να αποδεχτούν τα cookies ή όχι. Ωστόσο, η μη αποδοχή οδηγεί και στον περιορισμό των χρηστών από την ολοκληρωμένη πρόσβαση στον ιστότοπο και την πλήρη χρήση των υπηρεσιών που προσφέρονται.

Τα δεδομένα προσωπικού χαρακτήρα μπορούν να συλλεχθούν και να επεξεργαστούν από την Τράπεζα της Ελλάδος υπό συγκεκριμένες προϋποθέσεις και όταν βασίζονται σε συγκεκριμένα νομικά θεμέλια. Τέτοιες βάσεις αποτελούν: α) η συναίνεση του υποκειμένου, β) η συμβατική σχέση, γ) η έννομη υποχρέωση, δ) η διαφύλαξη ζωτικού συμφέροντος φυσικού προσώπου, ε) το καθήκον δημόσιου συμφέροντος/ άσκηση δημόσιας εξουσίας από τον υπεύθυνο επεξεργασίας και στ) το έννομο συμφέρον. Σε κάθε περίπτωση η συγκατάθεση μπορεί να δοθεί και να ανακληθεί ανά πάσα στιγμή, σύμφωνα με την βούληση του χρήστη. Η ανάκληση έχει ως συνέπεια την παύση της επεξεργασίας των δεδομένων, ενώ η επεξεργασία που προηγήθηκε θεωρείται νόμιμη.

Τέλος, η αρχή προστασίας δεδομένων, υποχρεώνει τα πιστωτικά ιδρύματα να εφαρμόζουν τα GDPR με σαφήνεια και διαφάνεια, ενημερώνοντας τα υποκείμενα των δεδομένων ότι πρόκειται να συλλεχθούν και να χρησιμοποιηθούν με την μορφή της επεξεργασίας, τα προσωπικά τους δεδομένα. Η ενημέρωση αυτή αποσαφηνίζεται ότι κρίνεται απαραίτητο να γίνεται με απλότητα και σαφήνεια και καθημερινή γλώσσα, η οποία γίνεται αντιληπτή από τον μέσο πελάτη. Θα πρέπει, δηλαδή, να γίνεται

ενημέρωση συνοπτικά και κατανοητό ύφος και το περιεχόμενο της να καθίσταται εύκολα προσβάσιμο σε κάθε πελάτη, που επιθυμεί να προστρέξει για να το διαβάσει ξανά.

3.3. Εφαρμογή της προστασίας προσωπικών δεδομένων – Μελέτη περίπτωσης οι μεσαίες και μικρομεσαίες επιχειρήσεις

Η ανάγκη της προστασίας των προσωπικών δεδομένων από τις επιχειρήσεις, θεωρείται κρίσιμο ζήτημα. Η ψήφιση του Κανονισμού των GDPR αποτέλεσε την αρχή, σύμφωνα με την οποία θεσπίστηκαν οι βάσεις για την εφαρμογή των GDPR από τις μικρές και μεσαίες επιχειρήσεις, προστατεύοντας τα δεδομένα των ιδιωτών που κοινοποιούνται σε αυτές. Για την εφαρμογή τους, απαιτείται πρώτα η γνώση και στην συνέχεια η επιλογή του τρόπου εφαρμογής τους.

Μελετώντας περιπτώσεις επιχειρήσεων εντός της Ευρωπαϊκής Ένωσης, γίνεται εύκολα αντιληπτό, ότι υπάρχει μεγάλη έλλειψη ενημέρωσης, και συνάμα εφαρμογής της προστασίας των προσωπικών δεδομένων στις όλο και μικρότερες επιχειρήσεις, η οποία όμως γίνεται σημαντική προσπάθεια να βελτιωθεί ανά τα χρόνια.

Με βάση τον Lindgren, P. (2018), το μέγεθος της εταιρείας παίζει σημαντικό ρόλο κατά την εφαρμογή των GDPR, καθώς όσο μικρότερη είναι μια εταιρεία, τόσο μεγαλύτερες θα αποτελούν οι αλλαγές που πρέπει να προβούν. Μάλιστα, ο μεγάλος αριθμός μικρών εταιρειών, οι οποίες πασχίζουν να συμμορφωθούν καταδεικνύει τον αγώνα, που καταβάλλουν για να κατανοήσουν τις απαιτήσεις του Κανονισμού. **Η συμμόρφωση με τα GDPR αποδεικνύεται ότι αποτελεί ένα έξοδο, το οποίο απαιτεί πολύ χρόνο, καθώς απαιτεί χρηματικούς και ανθρώπινους πόρους, τους οποίους οι μικρές και μεσαίες επιχειρήσεις πασχίζουν να αποκτήσουν.**

Σύμφωνα με τους Freitas, da Silva, (2018), η πλειοψηφία των μικρών και μεσαίων επιχειρήσεων της Πορτογαλίας **δεν γνωρίζει** τον νέο κανονισμό για τα GDPR, ούτε και τον νόμο με τον οποίο εφαρμόστηκαν στην Πορτογαλία, με αποτέλεσμα οι επιχειρήσεις να μην έχουν συμμορφωθεί με τις νέες απαιτήσεις που έχουν ανακύψει για την προστασία προσωπικών δεδομένων. Ειδικότερα, σε έρευνα που πραγματοποιήθηκε σε μικρομεσαίες επιχειρήσεις που καλύπτουν το 99,9% των επιχειρήσεων της Πορτογαλίας, αποδείχθηκε ότι όλες αυτές οι εταιρείες και οι εργαζόμενοι αυτών που έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα **δεν διαθέτουν κατάλληλη ενημέρωση για τα καθήκοντα και τις υποχρεώσεις που πρέπει να ακολουθούν** σχετικά με την συγκατάθεση, τις αρχές επεξεργασίας σύμφωνα

με τον νέο κανονισμό, ενώ **δεν γνωρίζουν και την υποχρέωση** λογοδοσίας του υπευθύνου επεξεργασίας δεδομένων, ούτε και την υποχρεωτικότητα στην γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην Εποπτική Αρχή. Η άγνοια δε επεκτείνεται και στον τρόπο που θα εξασφαλίζουν την ασφαλή τήρηση, ήτοι την αποθήκευση και επεξεργασία των δεδομένων προσωπικού χαρακτήρα, καθώς και στα δικαιώματα των υποκειμένων των δεδομένων. Επιπλέον, οι εταιρείες δεν γνώριζαν ότι εφόσον αυτές συνάπτουν συμβάσεις με τρίτους, είναι αναγκαίο να συμμορφώσουν τις συμβάσεις με τα GDPR, όταν η παροχή των υπηρεσιών τους περιλαμβάνει τη συλλογή, αποθήκευση, πρόσβαση και επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με τους Koski & Valmari (2020), σε έρευνα που πραγματοποιήθηκε το 2018 σε επιχειρήσεις της ΕΕ έγινε αντιληπτό ότι **το κόστος** συμμόρφωσης με τα GDPR **είναι αυξημένο**, ενώ περίπου 500.000 ευρωπαϊκοί οργανισμοί προσέλαβαν υπεύθυνο προστασίας δεδομένων, με μέσο ετήσιο μισθό περίπου στις 80.000 ευρώ. Συνεπώς, δημιουργείται ένα επιπλέον κόστος περίπου 40 δισεκατομμυρίων ευρώ, μόνο με την απασχόληση ενός επιπλέον ατόμου. Η προσπάθεια συμμόρφωσης και η διατήρηση αυτής έχει αυξημένα κόστη, πλήττοντας οικονομικά τις εταιρείες που συλλέγουν και επεξεργάζονται δεδομένα. Επιπλέον, γίνεται αντιληπτό ότι επιχειρήσεις που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα, όπως είναι τα νοσοκομεία, έχουν μεγαλύτερο οικονομικό κόστος και περισσότερες αρνητικές συνέπειες από την εφαρμογή του Κανονισμού, καθώς η περίπτωση παραβίασης σε τέτοιου είδους περιπτώσεις, θα δημιουργήσει και ανάλογα πρόστιμα.

Σε μελέτη των Goldberg et al. (2019), που πραγματοποιήθηκε μεταξύ 1500 διαδικτυακών επιχειρήσεων αναδείχθηκε η αρνητική διάσταση στο ηλεκτρονικό εμπόριο και τις πωλήσεις μετά την επιβολή του Κανονισμού, καταγράφοντας μάλιστα και μείωση σχεδόν 10%.

Η έρευνα των Koski & Valmari (2020) αποτυπώνει την εξέλιξη στα περιθώρια κέρδους των ευρωπαϊκών και αμερικάνικων επιχειρήσεων, τα οποία δεν έχουν διαφοροποιηθεί πολύ σε σχέση με τα δεδομένα πριν τον Κανονισμό. Συγχρόνως, υπογραμμίζεται η μειονεκτικότερη θέση, στην οποία βρίσκονται οι μικρομεσαίες επιχειρήσεις της Ευρώπης σε σχέση με τις αμερικάνικες, αφού δεν υπάρχει εξέλιξη στα κέρδη τους.

Με βάση τους Buckley et al. (2021), το αντίκτυπο των GDPR στις επιχειρήσεις έχει θετικές και αρνητικές συνέπειες σε αυτές. Κάνοντας αναδρομή στο έτος 2019,

έρευνες καταδεικνύουν ότι οι μικρές επιχειρήσεις δεν πρόλαβαν ή δεν προσπάθησαν να συμμορφωθούν με τις αρχές του Κανονισμού. Τρία χρόνια μετά την εφαρμογή των GDPR, οι επιχειρήσεις είναι πια αρκετά δεκτικές στην νέα πραγματικότητα. Έχουν αντιληφθεί ότι τα οφέλη των GDPR πολλές φορές υπερτερούν και από τα κόστη της εφαρμογής αυτών. Το σημαντικότερο είναι ότι πλέον η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται με μεγαλύτερη διστακτικότητα και χωρίς υπερβολές, **θεωρώντας ότι πρέπει να μεταχειρίζονται τα δεδομένα των τρίτων, όπως τα δικά τους**. Μάλιστα, η πλειοψηφία των επιχειρήσεων της ΕΕ, έχει αυξήσει σημαντικά το προσωπικό της, ώστε να συμμορφωθεί με τον Κανονισμό. Επιπλέον, μελετώντας περιπτώσεις επιχειρήσεων στο Ηνωμένο Βασίλειο και την Ιρλανδία, γίνεται αντιληπτό ότι **κίνητρο στην διαδικασία αποτέλεσε ο φόβος της επιβολής των προστίμων**, αφού για σοβαρές παραβιάσεις μπορεί να ανέλθει μέχρι και τα 20 εκατ. ή έως και 4% του κύκλου εργασιών των επιχειρήσεων.

Η σημαντική **ευαισθητοποίηση που υπήρξε εντός των επιχειρήσεων**, τις εμποδίζει πια να σωρεύουν πλήθος δεδομένων, τα οποία δεν τους χρησιμεύουν. Σύμφωνα με τους Buckley et al. (2021), η εφαρμογή του Κανονισμού **συνδέθηκε άρρηκτα με την τεχνολογική τους εξέλιξη**, δημιουργώντας νέες υποδομές στην πληροφορική τους, ψηφιοποιώντας και αυτοματοποιώντας τα συστήματα, που χρησιμοποιούν. Η **αναδιάρθρωση στην οργάνωση**, προκειμένου να πραγματοποιείται αυστηρότερος έλεγχος στην πρόσβαση και επεξεργασία των δεδομένων, ώθησε αυτές στην **καινοτομία και στην εξέλιξη της τεχνογνωσίας τους, απασχολώντας και περισσότερο προσωπικό, με νομικό κυρίως υπόβαθρο**, το οποίο θα συμβάλλει στην συμμόρφωση τους. Οι ανωτέρω τεχνολογικές αλλαγές, θα δημιουργήσουν και θετικό αντίκτυπο στους πελάτες, οι οποίοι θα εμπιστευτούν την επιχείρηση πιο εύκολα, δημιουργώντας και την κατάλληλη φήμη, για την προσέλκυση περισσότερων ενδιαφερομένων.

Ωστόσο, **η πραγματικότητα διαφέρει για τις μικρομεσαίες επιχειρήσεις**, οι οποίες **δεν διαθέτουν τους πόρους να μπορέσουν να διασφαλίσουν την προστασία των δεδομένων και συγχρόνως να αυξήσουν την πελατεία τους**. Με την χρήση περισσότερων δεδομένων, μπορούσαν να υπεισέλθουν σε βαθύτερες γνώσεις για τους πελάτες και τα ενδιαφέροντα τους, προετοιμάζοντας τις καμπάνιες τους, και συγχρόνως προσελκύοντας νέους πελάτες. Η **ανάγκη κατηγοριοποίησης των πελατών που αναδύεται από τον Κανονισμό, εμποδίζουν την επικοινωνία** που υπήρχε παλαιότερα με αυτούς. Οι μικρομεσαίες επιχειρήσεις θεωρούν ότι η εφαρμογή και από τις ίδιες των

GDPR είναι υπερβολική και τους δημιουργεί **ανταγωνιστικό μειονέκτημα**, αφού δεν μπορούν να ανταπεξέλθουν **στα κόστη της συμμόρφωσης, τα οποία περιλαμβάνουν την πρόσληψη ειδικού προσωπικού, την τεχνολογική ανάπτυξη και την εξέλιξη του μάρκετινγκ. Σε περίπτωση δε παραβίασης δεδομένων, δημιουργείται ο κίνδυνος επιβολής υψηλού προστίμου, ο οποίος θα οδηγήσει σε κλονισμό της φήμης της επιχείρησης και ακόμη και στην καταστροφή της.**

Συνεπώς, ενώ έχει τεθεί ως ύψιστη ανάγκη η προστασία του απορρήτου των δεδομένων από τις επιχειρήσεις, αναδεικνύοντας τα οφέλη για τους καταναλωτές, παραμελείται η ύπαρξη ή μη οφελών στις εταιρίες, τα οποία θα μπορούσαν να δικαιολογήσουν την επένδυση σε διαδικασίες διαχείρισης δεδομένων και ασφάλειας. Κρίνεται επομένως αναγκαίο να υπάρξει διαχωρισμός των επιχειρήσεων ανάλογα με την δυναμική τους και αναλογική εφαρμογή του Κανονισμού σε σχέση με το πλήθος δεδομένων που επεξεργάζονται.

Σύμφωνα με τους Xuereb et al. (2019), η δυσκολία στην εφαρμογή των GDPR δεν εμφανίζεται μόνο στις μικρές επιχειρήσεις, αλλά και στα μικρά ευρωπαϊκά κράτη. Ειδικότερα, η Μάλτα, η Σλοβενία, το Λουξεμβούργο, η Λιθουανία, η Λετονία, η Εσθονία και η Κύπρος είναι χώρες εντός της ΕΕ, οι οποίες έχουν πληθυσμό λιγότερο από 3 εκατομμύρια. Με έρευνα που πραγματοποιήθηκε στα μικρά αυτά κρατίδια, επιβεβαιώθηκαν τα ανωτέρω, ήτοι αναδείχθηκε η αύξηση στο φόρτο εργασίας και στο κόστος κατά την συμμόρφωση με τα GDPR, παράλληλα όμως συνέβαλαν και στην ενίσχυση της εμπιστοσύνης των πελατών και την δημιουργία θετικής εικόνας (φήμης) στις επιχειρήσεις. Ωστόσο, στις περιπτώσεις αυτές το πρόβλημα εντοπίζεται στα υποκείμενα των δεδομένων, τα οποία αγνοούν σε μεγάλο βαθμό τον Κανονισμό, με αποτέλεσμα να είναι επιφυλακτικοί κατά την κοινοποίηση των στοιχείων τους. Επιπλέον, αναδύεται η προβληματικότητα στην ψήφιση και εφαρμογή του Κανονισμού, καθώς υπάρχουν ίδιοι όροι για διαφορετικές περιστάσεις, αφού προτάσσει την ίδια εφαρμογή από μικρομεσαίες και μεγάλες επιχειρήσεις, καθώς και μεταξύ μεγαλύτερων και μικρότερων κρατών της ΕΕ, θέτοντας σε μειονεκτική θέση τα μικρότερα κράτη και επιχειρήσεις, που δεν διαθέτουν την ίδια δυναμική και έκταση.

Ο Κανονισμός στην ελληνική κοινωνία δεν έχει την ίδια εφαρμογή σε σχέση με τις μικρομεσαίες επιχειρήσεις της ΕΕ. Σε πανελλαδική έρευνα που πραγματοποιήθηκε το Μάιο του 2018 από την Γενική Συνομοσπονδία Επαγγελματιών Βιοτεχνών Εμπόρων Ελλάδας, έγινε αντιληπτό ότι υπάρχει μεγάλη άγνοια από τις επιχειρήσεις σχετικά με την προστασία των δεδομένων και πως αυτές πρέπει να προσαρμοστούν

στον νέο Κανονισμό, υπογραμμίζοντας την ανάγκη ορθής ενημέρωσης και υποστήριξης των μικρομεσαίων επιχειρήσεων σχετικά με τα GDPR.

Σύμφωνα με την εταιρεία Accounting Solutions (2022), τρία σχεδόν χρόνια μετά την ψήφιση του Κανονισμού, έγινε μια σημαντική προσπάθεια κυρίως από τις μεγαλύτερες εταιρίες για να θωρακίσουν τα προσωπικά δεδομένα τόσο των εργαζομένων, όσο και των πελατών και των συνεργατών τους, εντάσσοντας στο δυναμικό τους τον υπεύθυνο επεξεργασίας δεδομένων. **Το μεγαλύτερο πρόβλημα εντοπίζεται στις νεοφυείς επιχειρήσεις και στις μικρές και μεσαίες επιχειρήσεις, οι οποίες βέβαια δεν έχουν την υποχρέωση για ορισμό ως υπεύθυνο επεξεργασίας δεδομένων τρίτο πρόσωπο, καθώς η επίβλεψη της επεξεργασίας γίνεται από τους ίδιους τους επιχειρηματίες ή το προσωπικό τους, εφόσον δεν επεξεργάζονται δεδομένα σε μεγάλη κλίμακα. Ωστόσο, υπάρχει υποχρέωση να ενημερωθούν οι επιχειρήσεις για το πότε και με ποιον τρόπο πρέπει να γίνεται η επεξεργασία των δεδομένων και σε ποιον βαθμό.**

Από τα ανωτέρω αναδύεται η έλλειψη ενημέρωσης και εφαρμογής του Κανονισμού από τις μικρές και μεσαίες επιχειρήσεις στην Ελλάδα, οι οποίες αποτελούν την ραχοκοκαλιά της ελληνικής οικονομίας και καλύπτουν το μεγαλύτερο ποσοστό των ελληνικών επιχειρήσεων. Αυτό καταδεικνύει την σημαντικότητα στην εφαρμογή του Κανονισμού από τις επιχειρήσεις αυτές, οι οποίες είναι εκτεθειμένες στον κίνδυνο της παράβασης των GDPR και στην επιβολή υψηλών προστίμων.

4. Ερευνητικό μέρος

4.1. Ερευνητικός σκοπός

Μετά την ολοκλήρωση της βιβλιογραφικής ανασκόπησης, μέσω της οποίας υπογραμμίστηκαν σημαντικά ζητήματα που αφορούν τα προσωπικά δεδομένα και την προστασία αυτών, ακολούθησε η διερεύνηση του θέματος από την σκοπιά των επιχειρήσεων, εμβαθύνοντας στις μικρό-μεσαίες επιχειρήσεις. Με βάση τα ανωτέρω αναδύθηκαν σημαντικά ερωτήματα τα οποία πρέπει να τεθούν προς έρευνα, που σχετίζονται με την συμμόρφωση των μικρών και μεσαίων επιχειρήσεων με τα GDPR στην Ελλάδα, το κόστος συμμόρφωσης και τον τρόπο επεξεργασίας των προσωπικών δεδομένων.

Ειδικότερα, τα ερευνητικά ερωτήματα είναι τα εξής:

- Μετά τον Νέο Κανονισμό για τα GDPR, με ποιον τρόπο οι μικρές και μεσαίες επιχειρήσεις συλλέγουν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα;
- Γιατί οι μικρομεσαίες επιχειρήσεις δεν έχουν συμμορφωθεί με τον Κανονισμό; Ποια προβλήματα αντιμετωπίζουν;

4.2. Ερευνητική μεθοδολογία

Σύμφωνα με την Kothari (2004), η έρευνα αποτελεί μία μέθοδο, μέσω της οποίας θα ακολουθήσει μια διαδικασία, η οποία θα οδηγήσει στο να αποκτηθεί νέα γνώση. Σκοπός της έρευνας τίθεται να ευρεθούν οι απαντήσεις στα ερευνητικά ερωτήματα, που θέτει ένας ερευνητής, με την εφαρμογή συγκεκριμένων επιστημονικών διαδικασιών. Οι βασικές μέθοδοι έρευνας είναι η ποσοτική και η ποιοτική. Υπάρχει δε και η μικτή μέθοδος, σύμφωνα με την οποία συνδυάζονται οι δύο βασικοί μέθοδοι ερευνών. Για την συγκεκριμένη εργασία, θα χρησιμοποιηθεί η ποιοτική έρευνα.

4.3. Ερευνητικό εργαλείο

Οι συνεντεύξεις αποτελούν ένα εργαλείο έρευνας, το οποίο χρησιμοποιείται προκειμένου να συλλεχθούν οι κατάλληλες πληροφορίες, οι οποίες δεν είναι διαθέσιμες στη βιβλιογραφία και μέσω της παρατήρησης. Πρόκειται για μια διαδικασία, η οποία πραγματοποιείται μεταξύ δύο ατόμων, στα πλαίσια της κοινωνικής αλληλεπίδρασης, όπου η μία πλευρά, δηλαδή ο συνεντευκτής στοχεύει να αντλήσει πληροφορίες από το άλλο μέλος, τον ερωτώμενο. Το βασικότερο στην συνέντευξη αποτελεί ο σχεδιασμός αυτής, καθώς πρέπει να είναι με τέτοιο τρόπο διαμορφωμένη,

ώστε να εμπνέει εμπιστοσύνη στον ερωτώμενο, προκειμένου να εξασφαλιστούν και οι καλύτερες δυνατές αξιόπιστες και έγκυρες απαντήσεις του τελευταίου. Οι συνεντεύξεις επίσης, μπορεί να είναι τριών ειδών, ήτοι οι μη δομημένες, οι ημιδομημένες και οι δομημένες. Ως μη δομημένες θεωρούνται οι ανεπίσημες συζητήσεις, όπου οι ερωτήσεις προκύπτουν αυθόρμητα, κατά τη φυσική αλληλεπίδραση. Οι ημιδομημένες συνεντεύξεις είναι αυτές που κινούνται γύρω από ένα βασικό σενάριο ερωτήσεων, αλλά διευρύνονται με δευτερεύουσες ερωτήσεις με βάση τις απαντήσεις του εκάστου ερωτώμενου. Τέλος, στην δομημένη συνέντευξη ακολουθούνται συγκεκριμένες ερωτήσεις, οι οποίες είναι κοινές και προκαθορισμένες, προς όλους τους ερωτώμενους. Σε κάθε περίπτωση, οι ερωτήσεις πρέπει να είναι αμερόληπτες και σαφείς και να μην προσπαθούν να κατευθύνουν τον ερωτώμενο προς μία απάντηση/κατεύθυνση. Σχετικά με τις απαντήσεις, αυτές μπορεί να είναι ανοικτού τύπου ή να προκαθορίζονται από ένα σύνολο πιθανών απαντήσεων, μεταξύ των οποίων ο ερωτώμενος δύναται να διαλέξει την καταλληλότερη σύμφωνα με την δική του κρίση.

Στην εν λόγω έρευνα θα επιλέξουμε ως μορφή την ποιοτική δομημένη συνέντευξη, όπου θα προκαθορίζονται κάποιες από τις ερωτήσεις. Επιλέγονται, δηλαδή, οι ανοικτού τύπου απαντήσεις, από τις οποίες θα προκύψουν και άλλες ερωτήσεις, οι οποίες θα βοηθήσουν ώστε οι ερωτώμενοι να εκφραστούν με τον καλύτερο δυνατό τρόπο, αποτυπώνοντας τις απόψεις και τις εμπειρίες τους. Μέσω αυτού του ερευνητικού εργαλείου, το οποίο επιτυγχάνεται πρόσωπο με πρόσωπο μεταξύ των δύο μερών, δύναται να συλλεχθούν πληροφορίες, μέσω της λεκτικής επικοινωνίας, αλλά και με τις κινήσεις του σώματος και του τόνου της φωνής. Επίσης, με τον τρόπο αυτό, μπορούν να διατυπωθούν και προβληματισμοί ή ανησυχίες του ερωτώμενου.

Σε μία ποιοτική δομημένη συνέντευξη, οι ερωτήσεις οφείλουν να είναι ανοικτές και αμερόληπτες, αποφεύγοντας την χρησιμοποίηση λέξεων, οι οποίες δύναται να επηρεάσουν τις απαντήσεις και να αποτυπώνονται με σαφήνεια. Στόχος αποτελεί η συλλογή πληροφοριών, οι οποίες σχετίζονται με τα ερευνητικά ερωτήματα, καθώς από τις απαντήσεις των ερωτώμενων δύναται να υπάρχουν και πληροφορίες, οι οποίες είναι μη αναμενόμενες και μη εύκολα μετρήσιμες.

Η μέθοδος της συνέντευξης πέρα από τα ανωτέρα θετικά, εμπεριέχει και ορισμένα μειονεκτήματα, τα οποία σχετίζονται με την επιρροή που μπορεί να ασκήσει ο συνεντευκτής στον ερωτώμενο. Επιπροσθέτως, πρέπει να συνυπολογιστεί το κόστος μετακίνησης που απαιτείται, καθώς και ο χρόνος που είναι αναγκαίος τόσο για την

διεξαγωγή των συνεντεύξεων, όσο και για την απομαγνητοφώνηση. Σε κάθε όμως περίπτωση, η διαδικασία της συνέντευξης βοηθά στην παροχή διευκρινήσεων τόσο για τις ερωτήσεις, όσο και για τις απαντήσεις.

4.4. Ερευνητικό δείγμα

Οι συνεντεύξεις πραγματοποιήθηκαν σε 10 μικρομεσαίες επιχειρήσεις της Περιφέρειας Θεσσαλίας και της Στερεάς Ελλάδας. Όλες οι επιχειρήσεις που αποτελούν δείγμα της έρευνας απασχολούν πάνω από 15 εργαζόμενους, και συγκεκριμένα συμμετείχαν:

Πρακτορείο με ασφαλιστικές υπηρεσίες/προϊόντα	• 15 άτομα προσωπικό πλήρους απασχόλησης με πτυχίο και 5 από αυτούς έχουν και μεταπτυχιακό • DPO (διορισμένος + απασχόληση εντός της επιχείρησης) • Συνέντευξη με DPO
Εταιρεία παροχής υπηρεσιών οδικής βοήθειας	• 17 άτομα προσωπικό πλήρους απασχόλησης, από τους οποίους οι 9 διαθέτουν πτυχίο πανεπιστημίου και 2 από αυτούς έχουν και μεταπτυχιακό • DPO - επιχειρηματίας • Συνέντευξη με νόμιμο εκπρόσωπο- επιχειρηματία
Ξενοδοχειακή μονάδα 180 κλινών με εστίαση, χώρους εκδηλώσεων και σπα	• 30 άτομα προσωπικό (20 πλήρους και 10 μερικής απασχόλησης) από τους οποίους οι 15 διαθέτουν πτυχίο ΑΕΙ/ΤΕΙ και 2 από αυτούς έχουν και μεταπτυχιακό • DPO - επιχειρηματίας • Συνέντευξη με επιχειρηματία
Επιχείρηση με δραστηριότητα στα logistics φαρμάκων	• 31 άτομα προσωπικό (30 πλήρους και 1 μερικής απασχόλησης) - η πλειοψηφία είναι κάτοχοι πτυχίου, ενώ μόνο ένας έχει και μεταπτυχιακό. • DPO (διορισμένος + απασχόληση εντός της επιχείρησης) • Συνέντευξη με υπεύθυνο IT , ο οποίος είναι και ο DPO της επιχείρησης
Επιχείρηση με δραστηριότητα την παροχή υπηρεσιών ύδρευσης και αποχέτευσης	• 50 εργαζόμενους πλήρους απασχόλησης • DPO (διορισμένος + απασχόλησης εκτός επιχείρησης) • Συνέντευξη με DPO
Ιδιωτικός παιδικός σταθμός & νηπιαγωγείο	• 60 εργαζόμενους (50 πλήρους απασχόλησης και 10 μερικής απασχόλησης), από τους οποίους οι 50 έχουν πτυχίο και οι 15 από αυτούς διαθέτουν και μεταπτυχιακό • DPO (διορισμένος + απασχόληση εντός της επιχείρησης) • Συνέντευξη με τον υπεύθυνο εκπαίδευσης, ο οποίος είναι και DPO
Βιομηχανία ξύλινων κουφωμάτων	• 70 εργαζόμενους (60 πλήρους απασχόλησης και 10 μερικής απασχόλησης) από τους οποίους μόλις 10 έχουν πτυχίο και 2 διαθέτουν και μεταπτυχιακό • DPO - επιχειρηματίας • Συνέντευξη με την υπεύθυνη πωλήσεων
Επιχείρηση με δραστηριότητα την εμφιάλωση φυσικού μεταλλικού νερού	• 97 άτομα προσωπικό (96 πλήρους απασχόλησης και 1 μερικής απασχόλησης), από τους οποίους περίπου 40 άτομα διαθέτουν πτυχίο και 5 από αυτούς μεταπτυχιακό • DPO (διορισμένος + απασχόληση εντός της επιχείρησης) • Συνέντευξη με την υπεύθυνη HR, η οποία είναι και Operating Director & DPO της επιχείρησης
Λιανικό εμπόριο & χονδρική πώληση ειδών super market	• 120 άτομα προσωπικό πλήρους απασχόλησης, από τα οποία μόλις 15 διαθέτουν πτυχίο πανεπιστημίου και από αυτούς μόνο 2 έχουν και μεταπτυχιακό • DPO - επιχειρηματίας • Συνέντευξη με τον πρόεδρο της εταιρείας
Εταιρία τροφίμων: Παραλαβή πρώτης υλής - επεξεργασία και αποθήκευση σε ασηπτικούς σάκους και βαρέλια & επεξεργασία, συσκευασία και τυποποίηση προϊόντος	• 185 άτομα προσωπικό (183 πλήρους απασχόλησης και 2 μερικής απασχόλησης), από τους οποίους οι 65 διαθέτουν πτυχίο, και από αυτούς οι 12 έχουν και μεταπτυχιακό και περίπου 70-75 διαθέτουν βεβαίωση αναγγελίας από την διεύθυνση βιομηχανίας. • DPO (διορισμένος + απασχόληση εντός της επιχείρησης) • Συνέντευξη με την Διευθύντρια ανθρώπινου δυναμικού & DPO

Με βάση την πολυπλοκότητα του Κανονισμού για την προστασία δεδομένων, επιλέχθηκαν ορισμένες ερωτήσεις για την διενέργεια συνέντευξης, σύμφωνα με τις οποίες μπορεί να εκτιμηθεί ο τρόπος και ο βαθμός συμμόρφωσης των επιχειρήσεων, καθώς και αν προβαίνουν σε διαδικασίες προσαρμογής στα κρισιμότερα ζητήματα του νέου Κανονισμού. Συγκεκριμένα, η διερευνητική μελέτη πραγματοποιήθηκε με προσωπική συνέντευξη με ανώτερα στελέχη από την κάθε μικρομεσαία επιχείρηση. Οι συνεντεύξεις ηχογραφήθηκαν για απομαγνητοφώνηση και στην συνέχεια καταστράφηκαν, ώστε να διασφαλιστεί η ανωνυμία των συνεντευξιζόμενων και των εταιρειών. Ο χρόνος πραγματοποίησης της έρευνας – συνέντευξης ήταν στα τέλη του Σεπτεμβρίου και στις αρχές Οκτωβρίου του έτους 2024. Η συνέντευξη αποτέλεσε την καταλληλότερη μέθοδο, η οποία μπορούσε να χρησιμοποιηθεί, καθώς ήταν άμεση και επέτρεπε σε κάποιους από τους ερωτώμενους να λαμβάνουν και περαιτέρω πληροφορίες σχετικά με την κάθε ερώτηση.

4.5. Αποτελέσματα έρευνας - Συζήτηση



Σχήμα 4.5.1.

Στο ανωτέρω Σχήμα (βλ. Σχήμα 4.5.1.) γίνεται ανάλυση των τεσσάρων βασικών θεμάτων σχετικά με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, που αφορούν την γνώση, την συγκατάθεση, τις αρχές επεξεργασίας και το μητρώο δραστηριοτήτων επεξεργασίας. Αναλυτικότερα, και με βάση την συνέντευξη, οι 9/10 επιχειρήσεις γνώριζαν ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων τέθηκε σε ισχύ στις 25 Μαΐου 2018 και ήδη οι 4 από αυτές τον έθεσαν σε ισχύ την ίδια χρονιά, ενώ οι υπόλοιπες μεταγενέστερα και συγκεκριμένα τα έτη 2020 και 2021. Μόνο μία

από τις επιχειρήσεις δεν γνώριζε πότε ακριβώς τέθηκε σε ισχύ ο Κανονισμός, αλλά ξεκίνησε την εφαρμογή του το έτος 2020. Συγκεκριμένα, η κ. Καλλιόπη επεσήμανε:

«Δεν γνώριζα ότι ο Κανονισμός τέθηκε σε ισχύ τον Μάιο του 2018, αλλά τον θέσαμε σε εφαρμογή στην επιχείρηση από το 2021.»

Σε αντίθεση δηλαδή με την ανωτέρω μελέτη των Freitas, da Silva, (2018), σύμφωνα με την οποία οι περισσότερες μικρομεσαίες επιχειρήσεις στην Πορτογαλία δεν γνωρίζουν τον Κανονισμό και δεν τον έχουν εφαρμόσει, στην Ελλάδα μέσω ενός μικρού δείγματος επιχειρήσεων, έγινε αντιληπτό ότι υπάρχει γνώση του Κανονισμού και μάλιστα η πλειοψηφία αυτών τον εφαρμόζει.

Όλες οι επιχειρήσεις, οι οποίες συμμετείχαν στην έρευνα, διέθεταν επίσημη γραπτή συγκατάθεση για τα προσωπικά δεδομένα, η οποία αποτυπώνεται με σαφήνεια και απλότητα. Συγκεκριμένα, όλες οι επιχειρήσεις διαθέτουν πρότυπα συμβάσεων, εναρμονισμένα με τα GDPR, τα οποία είτε υπογράφονται από το προσωπικό κατά την πρόσληψη, ως επιπλέον παράρτημα στην σύμβαση εργασίας, ή αποτελούν ξεχωριστό έντυπο, το οποίο δίνεται σε πελάτες, ώστε να αποδέχονται την επεξεργασία των δεδομένων στα πλαίσια της δραστηριότητας των επιχειρήσεων και τίθενται σε πλήρη έλεγχο από τους ίδιους, ώστε να επιβεβαιώνουν την συγκατάθεση. Μάλιστα, ο κ. Νίκος, ο οποίος έχει την αρμοδιότητα του DPO της επιχείρησης ανέφερε ότι:

«Θα τεθεί από τον επόμενο μήνα και η ηλεκτρονική μορφή συγκατάθεσης, διότι όλα πλέον τείνουν να γίνουν ψηφιακά και με τον ίδιο τρόπο έχουμε πάρει και εμείς μία πλατφόρμα, που θα λαμβάνει ο πελάτης ένα SMS, θα πατάει το URL που θα λαμβάνει και θα υπογράφει στο κινητό του την συναίνεση ή όχι, λαμβάνοντας στο email τα αντίστοιχα έντυπα συγκατάθεσης.»

Με βάση την γραπτή συγκατάθεση, ο DPO ενός ιδιωτικού εκπαιδευτηρίου με τον οποίο έγινε συνέντευξη, ανέφερε ότι:

«Εξωτερικά, ως προς τα social media, στα οποία κάνουμε αναρτήσεις φωτογραφιών από εκδηλώσεις, δράσεις ή στιγμιότυπα της καθημερινότητας, πάντα κάνουμε επεξεργασία των φωτογραφιών, ώστε να μην φαίνονται τα πρόσωπα των παιδιών και να είναι καλυμμένα. Εσωτερικά, υπάρχει μια εφαρμογή που χρησιμοποιείται από την επιχείρηση, μέσα από την οποία κάνουμε εβδομαδιαία ανάρτηση, ώστε να ενημερώνονται οι γονείς για το πρόγραμμα και τις δράσεις του παιδιού τους στο σχολείο ανά εβδομάδα. Σε αυτή την περίπτωση οι γονείς συμπληρώνουν ένα έγγραφο συμφωνίας, όπου επιτρέπουν να ανεβαίνουν φωτογραφίες με το πρόσωπο του παιδιού στην «ψηφιακή τάξη» και να τις βλέπουν μόνο οι γονείς του τμήματος. Αν κάποιος γονέας έχει θέμα, δεν

ανεβαίνει μόνο το παιδί του, δημιουργώντας κώλυμα ιδίως στην περίπτωση των σχολικών εορτών. Μάλιστα, είχε γίνει επανάληψη σχολικής εορτής, προκειμένου να μην συμπεριληφθεί και φαίνεται το παιδί του γονέα, που διαφωνεί με την ανάρτηση αυτού. ».

Λόγω του Κανονισμού και των περιορισμών που τίθενται από αυτόν, όλες οι επιχειρήσεις απάντησαν ότι συλλέγουν μόνο τα απαραίτητα προσωπικά δεδομένα, που σχετίζονται με τους σκοπούς τους, ή και κάποιες φορές λιγότερα και από αυτά που χρειάζονται, προκειμένου να μην σωρεύουν πλήθος δεδομένων ασκόπως.

Σε σύμπνοια επομένως με την ανωτέρω μελέτη των Buckley et al. (2021), και στις λοιπές ευρωπαϊκές πόλεις υπάρχει μεγάλος περιορισμός των δεδομένων που συλλέγονται, αφού όπως χαρακτηριστικά αναφέρεται *«μεταχειρίζονται τα δεδομένα τρίτων, όπως τα δικά τους δεδομένα»*.

Περαιτέρω σχετικά με την ύπαρξη επικαιροποιημένου καταλόγου για τις κάμερες παρακολούθησης, οι 5/10 επιχειρήσεις ανέφεραν ότι έχουν κάμερες στις εγκαταστάσεις τους και διατηρούν επικαιροποιημένο κατάλογο, οι 3/10 επιχειρήσεις επεσήμαναν ότι ενώ έχουν κάμερες στις εγκαταστάσεις τους δεν διαθέτουν επικαιροποιημένο κατάλογο, ενώ οι 2/10 επιχειρήσεις ανέφεραν ότι δεν διαθέτουν καθόλου κάμερες παρακολούθησης στις εγκαταστάσεις τους. Όλες οι επιχειρήσεις ανέφεραν ότι δεν κάνουν καταγραφή των κλήσεων τους, πλην μίας, η οποία κάνει μεν καταγραφή κλήσεων, καθώς επικοινωνεί με πλήθος πελατών και προμηθευτών τηλεφωνικώς, χωρίς όμως να διατηρεί επικαιροποιημένο κατάλογο, στον οποίον να συμπεριλαμβάνονται οι τηλεφωνικοί αριθμοί, των οποίων οι κλήσεις καταγράφονται.

Στα πλαίσια του ελέγχου των επιχειρήσεων, οι 7/10 επιχειρήσεις ανέφεραν ότι ο οργανισμός παρακολουθεί την χρήση της εταιρικής διεύθυνσης ηλεκτρονικού ταχυδρομείου (email), όπως και των διαδικτυακών ιστότοπων που εισέρχεται το προσωπικό της, μέσω ειδικού server, ενώ μόνο 3 από αυτές δεν προβαίνουν σε έλεγχο των ανωτέρω. Συγκεκριμένα η κ. Φωτεινή ως Διευθύντρια Ανθρώπινου Δυναμικού και DPO της επιχείρησης ανέφερε:

«Δεν γίνεται παρακολούθηση του email. Δίνονται προσωπικοί κωδικοί, τους οποίους επιλέγει ο ίδιος ο εργαζόμενος και σε περίπτωση που μπλοκάρει, το ξεμπλοκάρισμα θα πρέπει να γίνει με την παρουσία του εργαζομένου στο desktop ή στο laptop του και όχι διαδικτυακά και από απόσταση από τον υπεύθυνο IT της εταιρείας.».

Σε κάθε όμως περίπτωση, όλες οι επιχειρήσεις έχουν προβεί σε ενημέρωση των υπαλλήλων τους σχετικά με την χρήση των μέσων επικοινωνίας. Για την αποφυγή δε παραλείψεων ή κινδύνων παραβίασης των δεδομένων, όλες οι επιχειρήσεις διαθέτουν

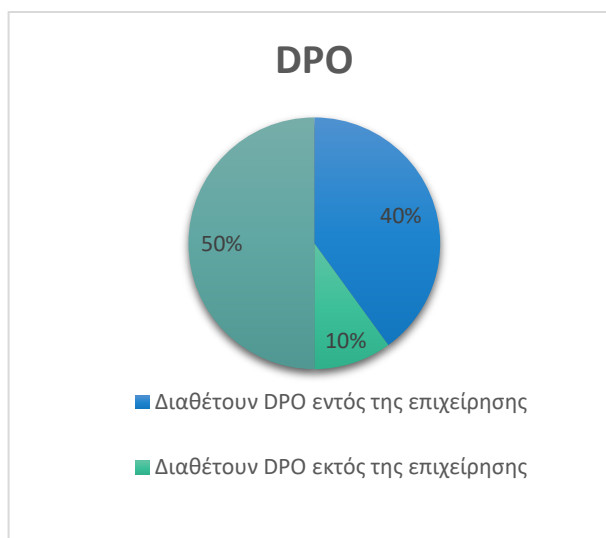
τα κατάλληλα εργαλεία μέσω των οποίων διασφαλίζεται η ασφάλεια και η εμπιστευτικότητα των προσωπικών δεδομένων. Τέτοια εργαλεία αποτελούν είτε τα ειδικά προγράμματα που διαθέτουν οι επιχειρήσεις, είτε κρυπτογραφήσεις δεδομένων και είσοδο σε αυτά με κωδικό, είτε με κάποια σχετικά κείμενα, τα οποία περιλαμβάνουν ειδικά μέτρα προστασίας που πρέπει να λαμβάνονται, σύμφωνα με τον Κανονισμό. Τέσσερις μάλιστα από τις επιχειρήσεις ανέφεραν ότι διαθέτουν σύστημα διαβαθμισμένης πρόσβασης, μέσω του οποίου αποκλείονται κάποιοι υπάλληλοι από την πρόσβαση σε ορισμένα δεδομένα, ενώ όσο αυξάνεται η βαθμίδα της θέσης του ατόμου στην εταιρεία, τόσο αυξάνεται και η πρόσβαση στα δεδομένα. Η πλήρης δε πρόσβαση παρέχεται κυρίως στα ανώτερα στελέχη των εταιρειών. Ειδικότερα, η κ. Φωτεινή αναφέρει:

«Έχουν πραγματοποιηθεί και εκπαιδεύσεις για την ασφάλεια στον κυβερνοχώρο και μέσα σε αυτά είχε ενταχθεί και η ασφάλεια των προσωπικών δεδομένων. Αυτό που είχε γίνει σαφές είναι ότι ο υπολογιστής και το κινητό τηλέφωνο είναι για καθαρά εταιρικούς σκοπούς και η εταιρεία δεν φέρει οποιαδήποτε ευθύνη αν ο εργαζόμενος κάνει και χρήση προσωπικών δεδομένων. Δηλαδή αν εγώ στον υπολογιστή μου αποθηκεύσω και δικές μου φωτογραφίες και αυτές χαθούν επειδή χάλασε ο σκληρός δίσκος, η εταιρεία δεν φέρει καμία απολύτως ευθύνη παρά μόνο για τα εταιρικά δεδομένα που είναι αποθηκευμένα στον υπολογιστή. Τα back up παίρνονται από τον χρήστη, κρυπτογραφημένα από κεντρικό server της εταιρείας, όπου μόνο ο ίδιος ο χρήστης μπορεί να τα επαναφέρει αν το επιθυμεί... Επιπλέον υπάρχει διαβάθμιση ρόλων, ή όπως την λέμε εμείς διαβαθμισμένη πρόσβαση, δηλαδή ο κάθε εργαζόμενος ανάλογα με την θέση που κατέχει του δίνεται και η αντίστοιχη πρόσβαση. Για παράδειγμα σε κάποια δεδομένα συνταγών, ο εργαζόμενος που δουλεύει στο χημείο, δεν μπορεί να εκτυπώσει, δεν μπορεί να κάνει αντιγραφή, μπορεί μόνο να κάνει ανάγνωση. Ο προϊστάμενος ποιοτικού ελέγχου μπορεί και να εκτυπώσει και ο διευθυντής μπορεί και να κάνει αντιγραφή. Δηλαδή η διαβαθμισμένη πρόσβαση έρχεται και διασφαλίζει στα πλαίσια του δυνατού την εταιρεία.».

Σχετικά με τον μέγιστο χρόνο απόκρισης, στις 8 επιχειρήσεις καθορίζεται ρητώς, ενώ στις υπόλοιπες 2 επιχειρήσεις δεν γίνεται καθορισμός αυτού. Επιπλέον, οι 7 επιχειρήσεις διαθέτουν μητρώο διαδικασίας αναφοράς σε τρίτους και μόνο 3 δεν διαθέτουν καθόλου το συγκεκριμένο μητρώο. Όλες όμως οι επιχειρήσεις ανέφεραν ότι δίνεται η δυνατότητα σε οποιοδήποτε υποκείμενο προστασίας δεδομένων θέλει να

προβεί σε διαγραφή, διόρθωση ή εναντίωση στην επεξεργασία, να το ζητήσει αυτό έστω και προφορικά από την επιχείρηση. Ωστόσο, ουδέποτε έτυχε να συμβεί.

Αν και όλες οι επιχειρήσεις απασχολούν λιγότερους από 250 υπαλλήλους, ήδη οι 5 από αυτές έχουν ορίσει Υπεύθυνο Προστασίας Δεδομένων (DPO), ενώ στις υπόλοιπες επιχειρήσεις ο ρόλος αυτός εκτελείται από τους ίδιους τους επιχειρηματίες. Σε περαιτέρω εμβάθυνση στο θέμα αυτό, οι 5 κυρίως επιχειρήσεις που έχουν ορίσει DPO ανέφεραν ότι αν και γνωρίζουν ότι στις μικρομεσαίες επιχειρήσεις δεν απαιτείται ο ορισμός ετέρου προσώπου, ο οποίος να αναλαμβάνει αυτό τον ρόλο, αυτές επέλεξαν να ορίζουν ήδη τρίτο πρόσωπο που είτε απασχολείται εντός της εταιρείας, είτε και εκτός αυτής. Αυτό πραγματοποιείται κυρίως προκειμένου να επιτυγχάνεται η συμμόρφωση με τον Κανονισμό, και



παράλληλα η επιχείρηση να βρίσκεται σε **Σχήμα 4.5.2.** παρακολούθηση και έλεγχο της συμμόρφωσης αυτής από τον DPO, καθώς και να συμβουλευόνται ή να ενημερώνονται για τυχόν αλλαγές που προκύπτουν από τον Κανονισμό. Επίσης, οι πολλαπλές αρμοδιότητες του επιχειρηματία δεν του επιτρέπουν να επιφορτίζεται και με αυτόν τον ρόλο, οπότε μεταθέτει τον έλεγχο αυτών σε τρίτους, κατάλληλα εκπαιδευμένους υπαλλήλους. Στην συζήτηση με τον κ. Ελευθέριο, ο οποίος έχει τον ρόλο του εξωτερικού DPO, δηλαδή δεν εργάζεται εντός της επιχείρησης, αναφέρει ότι:

«Αν και δεν απασχολεί η επιχείρηση πάνω από 250 εργαζόμενους, έχω οριστεί ως υπεύθυνος προστασίας δεδομένων, αφενός μεν διότι υπάρχουν αρκετά δεδομένα για διακίνηση, αφετέρου δε είναι ένα επιπλέον εθελοντικό βήμα που κάνει ο Οργανισμός, γιατί θέλει να υπάρχει πλήρης συμμόρφωση και να μην υπάρχει οποιαδήποτε έλλειψη πειθαρχίας».

Όπως και στο άρθρο των Buckley et al. (2021), που περιγράφεται παραπάνω, εφόσον έγινε αντιληπτή η θέση και ο ρόλος των προσωπικών δεδομένων στις επιχειρήσεις, υπήρξε αύξηση του προσωπικού, κυρίως με νομικό υπόβαθρο, προκειμένου να ενισχύσουν την προστασία των προσωπικών δεδομένων. Ωστόσο, σύμφωνα με τους Koski & Valmari (2020), η ανωτέρω αύξηση του προσωπικού είναι

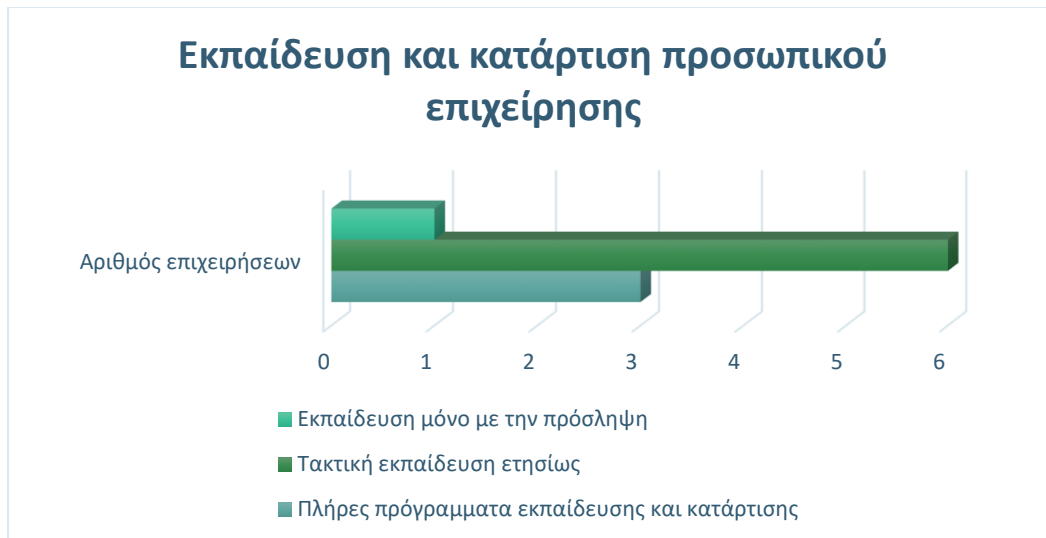
ασύμφορη για τις μικρομεσαίες επιχειρήσεις, αφού το κόστος των DPO υπερκαλύπτει τα έσοδα αυτών.

Σχετικά με τις επιχειρήσεις που συμμετείχαν στην έρευνα, οι 8 από αυτές, οι οποίες προβαίνουν σε υπογραφή συμβάσεων με τρίτους, ελέγχουν αν αυτές συμμορφώνονται με τα GDPR και μάλιστα οι 3 από αυτές διαθέτουν ειδικό τμήμα, και συγκεκριμένα το νομικό τμήμα της εταιρείας, το οποίο προβαίνει σε έλεγχο και διαμόρφωση αυτών σύμφωνα με τον Κανονισμό. Μόνο δύο από τις επιχειρήσεις, οι οποίες αν και προβαίνουν σε υπογραφή συμβάσεων με τρίτους, δεν έχουν προχωρήσει στον έλεγχο των συμβάσεων, σχετικά με το αν είναι συμμορφωμένες με τον Κανονισμό. Από όλες τις επιχειρήσεις, μόνο μία διαβιβάζει δεδομένα σε χώρες εκτός της Ευρωπαϊκής Ένωσης/ Ευρωπαϊκού Οικονομικού Χώρου, ελέγχοντας όμως πάντοτε την ύπαρξη νόμιμης άδειας σχετικά με την διαβίβαση στις χώρες αυτές. Μάλιστα, όπως η κ. Βάια, DPO της επιχείρησης υπογράμμισε:

« Στις συναλλαγές με αυτές τις χώρες, ο έλεγχος της άδειας, όπως και όλων των λοιπών παραμέτρων, είναι πολύ πιο τυπικός, λόγω της αυστηρότητας και του νομικού πλαισίου που ισχύει σε αυτές. ».

Σχετικά με την ενημέρωση των υπαλλήλων και την εκπαίδευση αυτών, όλες οι επιχειρήσεις επεσήμαναν ότι έχουν προβεί σε πλήρη ενημέρωση του προσωπικού που έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα. Μάλιστα, οι 9 από τις 10 επιχειρήσεις ανέφεραν ότι ακολουθούν τακτική και μόνιμη εκπαίδευση, η οποία κυρίως επαναλαμβάνεται μια φορά το χρόνο. Οι 3 δε από τις ανωτέρω 9 επιχειρήσεις ανέφεραν ότι πέρα από την τακτική εκπαίδευση, προβαίνουν και σε πλήρη πρόγραμμα σεμιναρίων και πιστοποιήσεων. Μόνο μια επιχείρηση ανέφερε ότι η ενημέρωση γίνεται μόνο κατά την πρόσληψη των υπαλλήλων, ενώ δεν έχει υιοθετηθεί από τον οργανισμό κάποιο πλήρες πρόγραμμα κατάρτισης, το οποίο να επαναλαμβάνεται σε τακτική βάση. Συγκεκριμένα, ο κ. Ελευθέριος, ο οποίος τελεί το ρόλο του εξωτερικού DPO της επιχείρησης ανέφερε ότι:

«Υπάρχει πλάνο ετήσιας εκπαίδευσης GDPR, το οποίο θα παρακολουθείται από τους εργαζόμενους. Μαζί με την ετήσια εκπαίδευση, θα γίνεται και αξιολόγηση σχετικά με την συμμόρφωση. Πέρα όμως από την τακτική εκπαίδευση, είχε γίνει επίσης και εκτάκτως εκπαίδευση προσωπικού, όταν έγινε αλλαγή του DPO, προκειμένου να υπάρχει επίγνωση του τι γνωρίζει το προσωπικό και ποια η ενημέρωση που έχει. ».



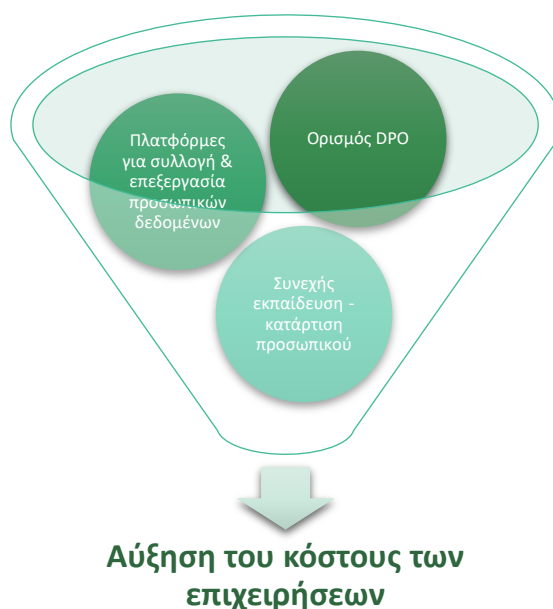
Σχήμα 4.5.3.

Επίσης, οι 9 από τις 10 επιχειρήσεις προβαίνουν σε τακτική αξιολόγηση της συμμόρφωσης της επιχείρησης με τους κανόνες και τους νόμους για τα GDPR, ενώ κάποιες από αυτές το κάνουν και με μεγαλύτερη συχνότητα κατά περίπτωση, όταν δηλαδή κρίνεται αναγκαίο. Μόνο μια επιχείρηση δεν προβαίνει στην τακτική αξιολόγηση, αγνοώντας πλήρως τον ρόλο του υπεύθυνου επεξεργασίας δεδομένων.

Σχετικά με την γνώση της υποχρέωσης γνωστοποίησης παραβιάσεων δεδομένων προσωπικού χαρακτήρα στην Εποπτική Αρχή, οι μισές επιχειρήσεις απάντησαν ότι γνώριζαν και διέθεταν γραπτή διαδικασία ειδοποίησης, ενώ οι υπόλοιπες αγνοούσαν την υποχρέωση ειδοποίησης της Αρχής Προστασίας Δεδομένων. Ωστόσο, σε καμία επιχείρηση ουδέποτε υπήρξε παραβίαση δεδομένων προσωπικού χαρακτήρα, πλην μιας, στην οποία εμφανίστηκε η περίπτωση του *fishing*, του λεγόμενου δηλαδή «ψαρέματος» πληροφοριών προσωπικού χαρακτήρα, ο οποίος όμως αποφεύχθηκε να ολοκληρωθεί, καθώς υπήρξε άμεση αντίδραση της εταιρείας, με παράλληλη ενημέρωση της Αρχής Προστασίας Δεδομένων. Συγκεκριμένα, ο κ. Νίκος υπογραμμίζει ότι:

«Υπάρχει γραπτή διαδικασία ειδοποίησης, με βάση την πολιτική που ακολουθούμε. Δεν έχει γίνει παραβίαση δεδομένων προσωπικού χαρακτήρα, εκτός από την απόπειρα που είχε γίνει για υποκλοπή των δεδομένων (fishing), λόγω λάθους από έναν υπάλληλο. Ευτυχώς διορθώθηκε άμεσα, αφού έγινε και η απαραίτητη αναγγελία στην προστασία δεδομένων. Ακολούθησε επιπλέον ενημέρωση και η επιχείρηση έθεσε την προσοχή ξανά στους εργαζομένους, σχετικά με την χρήση και την επεξεργασία των δεδομένων.».

Σχετικά με τα προβλήματα που αναδύονται ως προς την συμμόρφωση με τον Κανονισμό, οι 6 από τις 10 επιχειρήσεις ανέφεραν ότι το μέγεθος τους είναι τέτοιο, που δεν τους επιτρέπει να προβούν άμεσα σε περαιτέρω ενέργειες, ώστε να συμμορφωθούν πλήρως. Ειδικότερα, το κόστος της συμμόρφωσης είναι αυξημένο, σε σχέση με τα έσοδα των επιχειρήσεων, γεγονός που τους αποτρέπει από το λάβουν περαιτέρω μέτρα για την προστασία των δεδομένων. Εν αντιθέσει με τα ανωτέρω, οι υπόλοιπες 4 επιχειρήσεις λόγω των δεδομένων που επεξεργάζονται και της φύσεως των δραστηριοτήτων τους, έχουν αντιληφθεί την σημασία της συμμόρφωσης και προσπαθούν με κάθε μέσο να την πετύχουν. Ειδικότερα, οι 4/10 επιχειρήσεις έχουν προβεί σε ορισμό DPO εντός της επιχείρησης, έχουν συμμορφώσει τις συμβάσεις τους σε σχέση με τα GDPR και προβαίνουν σε τακτική ενημέρωση και κατάρτιση του προσωπικού τους.



Σχήμα 4.5.4

Από τις ερευνώμενες επιχειρήσεις, όλες γνώριζαν την πιθανότητα επιβολής προστίμου, λόγω της μη συμμόρφωσης με τον Κανονισμό, ωστόσο η πλειοψηφία αυτών δεν έχει αντιληφθεί την αυστηρότητα του πλαισίου του Κανονισμού, ούτε και το ύψος των προστίμων που δύναται να επιβληθεί.

Σε ταύτιση με την ανωτέρω μελέτη των Koski & Valmari (2020), το κόστος των επιχειρήσεων που αφορά την συμμόρφωση με τα GDPR είναι σημαντικό και αποτελεί ένα ακόμη έξοδο επιβαρυντικό για τις μικρότερες επιχειρήσεις, οι οποίες δύναται να το καλύψουν με δυσκολία.

Τέλος, η γνωστοποίηση στις ερευνώμενες επιχειρήσεις σχετικά με την υποχρέωση για την συμμόρφωση με τον Κανονισμό, δεν προήλθε από κρατικούς

φορείς, αλλά είτε από συλλόγους στους οποίους εντάσσονταν, είτε από άρθρα, ή από τους συμβούλους που διέθεταν, γεγονός που ανέδειξε την έλλειψη ενημέρωσης του Κράτους προς τις μικρομεσαίες επιχειρήσεις για τις υποχρεώσεις τους και τους κινδύνους που ελλοχεύουν η μη τήρησή τους.

Συνοψίζοντας, σύμφωνα με το πρώτο ερευνητικό ερώτημα, καταλήγουμε στο ότι οι μικρομεσαίες επιχειρήσεις συλλέγουν και επεξεργάζονται μόνο τα απαραίτητα σε αυτές προσωπικά δεδομένα, προκειμένου να επιτύχουν τους στόχους της δραστηριότητάς τους. Ο κίνδυνος παράβασης που απορρέει από τον Νέο Κανονισμό τις έχει καταστήσει αρκετά προσεκτικές, με το ποια και πόσα προσωπικά δεδομένα συλλέγουν, αντικαθιστώντας την παλαιά νοοτροπία, η οποία βασιζόταν στην ανεξέλεγκτη συλλογή δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με το δεύτερο ερώτημα της έρευνας, εμβαθύνοντας στα προβλήματα των επιχειρήσεων, αναδύεται ότι σε σύγκριση με τις μεγάλες επιχειρήσεις, οι μικρομεσαίες επιχειρήσεις αντιμετωπίζουν με διστακτικότητα την προστασία προσωπικών δεδομένων. Δεν δίνουν την απαραίτητη σημασία που απαιτείται στον τρόπο με τον οποίο πρέπει να αντιμετωπίζουν τις πληροφορίες, τις οποίες διοχετεύουν. Θεωρούν την λήψη μέτρων και την οργάνωση συγκεκριμένης πολιτικής περιττή, δίχως να διεισδύουν στην πηγή του προβλήματος. Το πρόβλημα αυτό έχει τις ρίζες του στην μη επαρκή και κατάλληλη ενημέρωση του κράτους προς τις μικρότερες επιχειρήσεις για την σημαντικότητα του Κανονισμού και την ανάγκη συμμόρφωσης με αυτόν. Η άγνοια των υποχρεώσεων των επιχειρήσεων και η ανεπαρκής ενημέρωση τις απομακρύνει από την υιοθέτηση των διατάξεων του Κανονισμού. Επιπροσθέτως, τα αυξημένα κόστη που απαιτούνται για την συμμόρφωση, σε συνδυασμό με την ήδη μεγάλη οικονομική επιβάρυνση που επιβάλλει συνεχώς η κυβέρνηση προς τις επιχειρήσεις, αναγκάζοντας τες να εισάγουν τα τελευταία δύο χρόνια νέα δεδομένα, λόγω φορολογικών και ασφαλιστικών αλλαγών, όπως είναι η υποχρεωτικότητα διασύνδεσης τερματικού POS και ταμειακής μηχανής, η ψηφιακή κάρτα, η υποχρεωτικότητα ασφάλισης των εγκαταστάσεων των επιχειρήσεων κα, δεν ευνοούν τις επιχειρήσεις, οι οποίες ακόμη και αν καταβάλλουν προσπάθεια για συμμόρφωση, με πραγματικά οικονομικά στοιχεία αδυνατούν. Ωστόσο, η μη συμμόρφωση και η πιθανότητα παράβασης των προσωπικών δεδομένων δύναται να προκαλέσει σημαντικότερα προβλήματα στην επιχείρηση, αφού ελλοχεύει ο κίνδυνος επιβολής προστίμου, το οποίο μπορεί να οδηγήσει και στο κλείσιμο αυτής, μη δυνάμενη να ανταποκριθεί οικονομικά.

5. Συμπεράσματα – Προτάσεις

Η προστασία των προσωπικών δεδομένων αποτελεί αναμφίβολα ένα δικαίωμα, που κατάφερε να θεμελιωθεί σε πανευρωπαϊκό επίπεδο. Αυτό επιτάχθηκε με την ισχύ του Κανονισμού της ΕΕ 679/2016, μέσω του οποίου επήλθαν σημαντικές αλλαγές στο χώρο της προστασίας των προσωπικών δεδομένων στις χώρες της Ευρωπαϊκής Ένωσης.

Η βιβλιογραφία γενικότερα καταδεικνύει το ρόλο της προστασίας των προσωπικών δεδομένων αλλά και το γεγονός ότι οι επιχειρήσεις έχουν υποχρέωση να ορίζουν Υπεύθυνο Προστασίας Δεδομένων (DPO) (Άρ. 37, παρ. 1 του Κανονισμού Προστασίας Προσωπικών Δεδομένων). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων ενίσχυσε σημαντικά την κατοχύρωση νέων δικαιωμάτων στα υποκείμενα των δεδομένων και επέβαλε νέες υποχρεώσεις στις επιχειρήσεις και τους υπεύθυνους επεξεργασίας, υπό το φάσμα της προστασίας της ιδιωτικότητας.

Μέσω της μελέτης περίπτωσης των μικρομεσαίων επιχειρήσεων, αναδύθηκαν τα θεμελιώδη και εναρκτήρια βήματα που πραγματοποιήθηκαν από αυτές, σχετικά με την συμμόρφωση με τον Νέο Κανονισμό. Αν και δεν υπήρξε επαρκή ενημέρωση προς τις επιχειρήσεις σχετικά με την ψήφιση και την εφαρμογή του Κανονισμού, οι ίδιες προσπάθησαν να ενημερωθούν και να προβούν στις κατάλληλες επιμορφώσεις και καταρτίσεις, προκειμένου να ανταπεξέλθουν στην νέα πραγματικότητα, που απαιτείται για την διαχείριση των δεδομένων προσωπικού χαρακτήρα.

Οι περιορισμοί της έρευνας ήταν ότι το δείγμα ήταν ενδεικτικό, αφού αφορούσε δέκα μικρομεσαίες επιχειρήσεις. Επίσης, η έρευνα πραγματοποιήθηκε σε συγκεκριμένη γεωγραφική έκταση και ειδικότερα σε επιχειρήσεις που έχουν έδρα την Θεσσαλία και την Στερεά Ελλάδα. Στις 10 επιχειρήσεις που μελετήθηκαν, έγινε αντιληπτό ότι δεν υπήρχε πλήρη συμμόρφωση και έλεγχος όλων των παραμέτρων του Κανονισμού, υπογραμμίζοντας τις ελλείψεις που υπάρχουν και τα βήματα που πρέπει να γίνουν, ώστε να εκπληρωθεί ο σκοπός της πλήρους συμμόρφωσης και προστασίας των δεδομένων.

Όλα τα ανωτέρω στηρίζονται στις συνεντεύξεις – συζητήσεις που πραγματοποιήθηκαν με ανώτατα στελέχη των επιχειρήσεων, οι οποίοι μέσω των απαντήσεων τους, προσπάθησαν να περιγράψουν την πραγματική κατάσταση που υπάρχει στις επιχειρήσεις αυτές.

Οι ανωτέρω περιορισμοί στην έρευνα, γεννούν προτάσεις προς διερεύνηση. Συγκεκριμένα, προτείνεται η διενέργεια έρευνας σε περισσότερες επιχειρήσεις σε ολόκληρη την επικράτεια, προκειμένου να γίνει αντιληπτό αν και κατά πόσο οι μικρομεσαίες επιχειρήσεις στην Ελλάδα γνωρίζουν τα GDPR και έχουν συμμορφωθεί με αυτά. Η διερεύνηση σε ευρύτερο πεδίο του ανωτέρω ζητήματος δύναται να αποτυπώσει με μεγαλύτερη ακρίβεια την πραγματική κατάσταση που ισχύει, καθώς έως σήμερα δεν έχουν συγγραφεί μελέτες και άρθρα που να περιγράφουν το πόσο έχουν συμμορφωθεί οι επιχειρήσεις και ποια προβλήματα αντιμετωπίζουν κατά την συμμόρφωση.

Μέχρι σήμερα έχει δημιουργηθεί ένας σημαντικός όγκος βιβλιογραφίας γύρω από την προστασία των προσωπικών δεδομένων, ωστόσο παρατηρείται μεγάλο κενό στον τρόπο εφαρμογής του από τις μικρομεσαίες επιχειρήσεις. Τα πορίσματα της έρευνας καταδεικνύουν ότι υπάρχει σημαντική έλλειψη ενημέρωσης και καθοδήγησης των επιχειρήσεων προκειμένου να υπάρξει σύμπνοια με τον Κανονισμό. Εφόσον οι επιχειρήσεις δεν γνωρίζουν τις υποχρεώσεις και τα καθήκοντα τους σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα, είναι σημαντικό να καθοριστεί μία μεθοδολογία ή ένας οδηγός, ο οποίος να βοηθήσει τις επιχειρήσεις να συμμορφωθούν. Δεν έχει γίνει ακόμη αντιληπτή η δύναμη της πληροφορίας και πως αυτή έχει αποτελέσει οικονομικό αγαθό για τις επιχειρήσεις, μέσω της νέας τεχνολογίας και του διαδικτύου.

Εκτός των ανωτέρω, τα κόστη της συμμόρφωσης εντείνουν τις οικονομικές δυσκολίες των επιχειρήσεων με αποτέλεσμα οι μικρομεσαίες επιχειρήσεις να προχωρούν με μικρά και σημαντικά βήματα, τα οποία θα τους οδηγήσουν πιο κοντά στον στόχο της πλήρους συμμόρφωσης με τα GDPR. Ωστόσο, η συνειδητοποίηση από τις επιχειρήσεις, που συλλέγουν και επεξεργάζονται σημαντικό αριθμό προσωπικών δεδομένων, της ανάγκης ορισμού DPO, καταδεικνύει την προσπάθεια μείωσης των παραβάσεων που ελλοχεύουν. Ήδη, σύμφωνα με την έρευνα, ο ορισμός DPO στις 5 από τις 10 ανωτέρω μικρομεσαίες επιχειρήσεις υπογραμμίζει την αντίληψη του κινδύνου που ελλοχεύει, λόγω του αριθμού και της σημαντικότητας των δεδομένων που συλλέγονται. Με τον τρόπο αυτό, παρέχεται κίνητρο στα υποκείμενα δεδομένων προσωπικού χαρακτήρα να αποβάλλουν οποιονδήποτε ενδοιασμό και να συγκαταθέσουν στην συλλογή και επεξεργασία των δεδομένων τους. Περαιτέρω, η προσπάθεια για συνεχή επαγρύπνηση των υπαλλήλων των επιχειρήσεων μέσω εκπαιδεύσεων και καταρτίσεων, που γίνεται από την πλειοψηφία των επιχειρήσεων,

είτε με μεγαλύτερη συχνότητα και ένταση είτε σε ετήσια βάση, αποτελεί μία μέθοδο, μέσω της οποίας εθιστούν την προσοχή του προσωπικού και παράλληλα εμπνέουν τους πολίτες για κοινοποίηση των στοιχείων τους σε επιχειρήσεις, οι οποίες γνωρίζουν τις υποχρεώσεις τους και τον τρόπο διαχείρισης των δεδομένων. Επιπροσθέτως, η δημιουργία κλίματος ασφάλειας και εμπιστευτικότητας είναι σημαντική σε μία επιχείρηση, αφού συμβάλει στην οικοδόμηση της φήμης της, προωθώντας και τις συναλλαγές της, συνεπώς και αυξάνοντας την πελατεία της.

Με βάση τα ανωτέρω, προτείνεται, επίσης, η διερεύνηση του τρόπου με τον οποίο μπορούν οι επιχειρήσεις να εμπνεύσουν τους πολίτες να εμπιστευτούν την αποθήκευση και επεξεργασία των δεδομένων τους.

Συνοψίζοντας, κρίνεται αναγκαίο να υπογραμμιστεί ο στόχος, ο οποίος είναι η προάσπιση της ελεύθερης κυκλοφορίας των δεδομένων, με την τήρηση των κανόνων. Αυτό είναι και το πνεύμα του Νέου Κανονισμού για την προστασία προσωπικών δεδομένων και οφείλεται να προωθηθεί από τις επιχειρήσεις και να τηρηθεί από αυτές. Είναι δε απαραίτητο να εφαρμοστεί ένα σχέδιο για την τήρηση των διαδικασιών, το οποίο θα διασφαλίζουν την συμμόρφωση με τις νέες απαιτήσεις που ανακύπτουν από την προστασία προσωπικών δεδομένων. Μάλιστα, θα ήταν επιβοηθητικό να δημιουργηθεί από το κράτος ένα πρόγραμμα επιδότησης προς τις μικρομεσαίες επιχειρήσεις, προκειμένου να περιοριστεί το κόστος συμμόρφωσης σε βαθμό ανάλογο της δυναμικότητας της επιχείρησης. Η μείωση του κόστους, παράλληλα με την ανάδειξη της σημαντικότητας εφαρμογής του Κανονισμού, θα αποτελούσε τα θεμέλια για να επέλθει η συμμόρφωση των μικρομεσαίων επιχειρήσεων με τα GDPR.

ΠΑΡΑΡΤΗΜΑ Ι (ΟΔΗΓΟΣ ΣΥΝΕΝΤΕΥΞΗΣ)

A. Γενικές πληροφορίες για την επιχείρηση

- 1) Ποια είναι η επωνυμία της επιχείρησης και ποια η μορφή της;
- 2) Ποιο είναι το όνομα σας (συνεντευξιαζόμενου) και ποια η θέση σας στην επιχείρηση;
- 3) Ποιες είναι οι ευθύνες σας σχετικά με την «Προστασία δεδομένων προσωπικού χαρακτήρα» στον οργανισμό σας;
- 4) Ποιος είναι ο συνολικός αριθμός των εργαζομένων της επιχείρησης; Από αυτούς πόσοι είναι πλήρους και πόσοι μερικής απασχόλησης;
- 5) Ποιος είναι ο συνολικός αριθμός εργαζομένων στην επιχείρηση σας, οι οποίοι διαθέτουν πτυχίο ΑΕΙ/ΤΕΙ και από αυτούς πόσοι διαθέτουν μεταπτυχιακό ή διδακτορικό;
- 6) Ποια/ες είναι η σημαντικότερη δραστηριότητα της επιχείρησης σας; Προσδιορίστε τον τομέα, τις δραστηριότητες, τα προϊόντα και τις αγορές.
- 7) Ποια τμήματα αγοράς καλύπτουν;
- 8) Διενεργείτε και εξαγωγές ;
- 9) Ποιο είναι το έτος ίδρυσης της επιχείρησης;

B. Ερωτήσεις ομαδοποιημένες σχετικά με τα άρθρα του GDPR

Γνώση

1. Γνωρίζετε ότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων τέθηκε σε πλήρη ισχύ από τις 25 Μαΐου 2018; Εσείς από πότε τον υιοθετήσατε στην εταιρεία?

Συναίνεση (άρθρα 6, 7 και 13)

2. Θεωρείτε ότι ο οργανισμός σας διαθέτει επίσημη γραπτή συγκατάθεση από όλα τα προσωπικά δεδομένα, η οποία αποτυπώνεται με σαφήνεια και απλότητα; Αν ναι, πού το στηρίζεται αυτό; Αν όχι, από που δημιουργούνται τα προβλήματα;
3. Με βάση το γεγονός ότι ο νέος Κανονισμός προσπαθεί να ενισχύσει την έννοια της «συγκατάθεσης», εισάγοντας νέες προϋποθέσεις για την απόκτηση αυτής, έχει υπάρξει έλεγχος από τον οργανισμό σας σχετικά με το πώς και σε ποιες περιστάσεις λήφθηκε η συγκατάθεση των υποκειμένων των δεδομένων προσωπικού χαρακτήρα; Αν ναι, μπορείτε να διηγηθείτε κάποιον έλεγχο; Αν όχι γιατί δεν έγινε ο έλεγχος;

4. Θεωρείτε ότι όσα προσωπικά δεδομένα συλλέγετε, είναι απολύτως απαραίτητα για τους στόχους που συλλέγονται; Αν ναι γιατί; Και πόσα προσωπικά δεδομένα εσείς συλλέγετε; Αν όχι γιατί;

Μητρώο δραστηριοτήτων επεξεργασίας (άρθρο 30)

5. Διαθέτει ο Οργανισμός σας επικαιροποιημένο κατάλογο, στον οποίο να συμπεριλαμβάνονται όλες οι κάμερες παρακολούθησης των εγκαταστάσεων σας;
6. Έχετε στην διάθεση σας ενημερωμένο κατάλογο, ο οποίος να περιλαμβάνει όλους τους τηλεφωνικούς αριθμούς, των οποίων οι κλήσεις καταγράφονται;

Εργατική νομοθεσία (άρθρο 88)

7. Θεωρείτε ότι ο Οργανισμός παρακολουθεί τη χρήση του τηλεφώνου/ηλεκτρονικού ταχυδρομείου/του Διαδικτύου;
8. Έχει ο Οργανισμός σας ενημερώσει τους υπαλλήλους σχετικά με τους κανόνες προστασίας δεδομένων, ώστε να τεκμηριώνουν τη χρήση των μέσων επικοινωνίας για ιδιωτικούς σκοπούς;

Δικαιώματα των υποκειμένων των δεδομένων (άρθρα 15, 16, 17, 19, 20, 21 και 22)

9. Θεωρείτε ότι η τεκμηρίωση που απαιτείται σύμφωνα με το διαδικαστικό πρωτόκολλο, η οποία σχετίζεται με τα αιτήματα των υποκειμένων των δεδομένων (προσβασιμότητα, διόρθωση, εναντίωση στην επεξεργασία και ορισμό του προφίλ, διαγραφή, φορητότητα δεδομένων) που στοχεύει στην επιβολή των δικαιωμάτων, καθορίζει και τον μέγιστο χρόνο της απόκρισης;
10. Διατηρείτε μητρώο διαδικασίας αναφοράς σε τρίτους, που σχετίζεται με την διόρθωση, τη διαγραφή ή τον περιορισμό της επεξεργασίας δεδομένων, η οποία ζητείται από τα υποκείμενα των δεδομένων;

Υπεύθυνος προστασίας δεδομένων (άρθρα 37, 38 και 39)

11. Διαθέτει ο Οργανισμός σας περισσότερους από 250 υπαλλήλους; Εάν ναι, αποτελείται τον διορισμένο Υπεύθυνο Προστασίας Δεδομένων;

Ασφάλεια επεξεργασίας δεδομένων (άρθρο 32)

12. Θεωρείτε ότι ο Οργανισμός σας έχει τα απαραίτητα εργαλεία, σύμφωνα με τα οποία διασφαλίζεται η ασφάλεια και η εμπιστευτικότητα των προσωπικών σας δεδομένων, υπό την δική σας ευθύνη;

Συμβάσεις (άρθρο 28)

13. Σε περίπτωση υπογραφής συμβάσεων με τρίτους σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, έχει ο Οργανισμός σας προβεί σε έλεγχο

περί συμμόρφωσης των συμβάσεων αυτών με τον Νέο Κανονισμό για τα GDPR;

Διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες (άρθρα 44, 45, 46)

14. Σε περίπτωση που διαβιβάζετε δεδομένα σε χώρες, οι οποίες είναι εκτός της Ευρωπαϊκής Ένωσης/Ευρωπαϊκού Οικονομικού Χώρου, προβαίνετε στην επιβεβαίωση του αν υπάρχει νόμιμη άδεια περί διαβίβασης στις χώρες αυτές ή όχι;

Κατάρτιση (άρθρα 25, 28, 47)

15. Όσοι από τον Οργανισμό διαθέτουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα, είναι ενημερωμένοι για τις υποχρεώσεις τους;
16. Εφόσον με τον νέο Κανονισμό για τα GDPR απαιτείται από τους Οργανισμούς η απαραίτητη μόνιμη ή τακτική εκπαίδευση στο προσωπικό που έχει πρόσβαση στα προσωπικά δεδομένα, γνωρίζετε αν υπάρχει κάποιο σχέδιο κατάρτισης ή πρόκειται να εφαρμοστεί;

Ευθύνη του υπευθύνου επεξεργασίας δεδομένων (άρθρο 24)

17. Προβαίνετε σε τακτική αξιολόγηση περί της συμμόρφωσης ή μη με τους κανόνες και τους νόμους για την προστασία προσωπικών δεδομένων;

Κοινοποίηση παραβίασης προσωπικών δεδομένων στην εποπτική αρχή (άρθρο 33)

18. Σε περίπτωση που υπάρξει παραβίαση των προσωπικών δεδομένων, διαθέτετε γραπτή διαδικασία ειδοποίησης;

Προβλήματα επιχειρήσεων σχετικά με την συμμόρφωση

19. Γιατί δεν υπάρχει πλήρης συμμόρφωση με τον Κανονισμό;
20. Ποια προβλήματα αντιμετωπίζετε σχετικά με την συμμόρφωση με τον Κανονισμό;

Βιβλιογραφία

Αιτιολογική σκέψη Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΕΕ) 2016/679.

Ακριβοπούλου Χ., (2011), Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από τον φακό του δικαιώματος στην ιδιωτική ζωή, ΘΠΔΔ, 7/2011, σ. 679-691

Aldboush, H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, 11(3), 90.

Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences*, 11(8), 3678.

Buckley, G., Caulfield, T., & Becker, I. (2021). "It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years. *arXiv preprint arXiv:2110.11905*.

Dove, E. S. (2018), The EU general data protection regulation: implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, 46(4), 1013-1030

Freitas, M. D. C., & Mira da Silva, M. (2018), GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4), 30.

Ιγγλεζάκης, Ι. (2016), Η συγκατάθεση στο δίκαιο προστασίας προσωπικών δεδομένων από το συλλογικό έργο «Προσωπικά Δεδομένα. Ανάλυση- Σχόλια Εφαρμογή, επιμ. Κοτσαλή, Νομική Βιβλιοθήκη, .

Ιγγλεζάκης, Ι. (2018), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Interactive learning 3η έκδοση.

Ιγγλεζάκη, Ι. (2021), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679), Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, Interactive

Koski, H., & Valmari, N. (2020). Short-term Impacts of the GDPR on Firm Performance (No. 77). ETLA Working Papers.

Kothari, C. R. (2004), Research methodology: Methods and techniques. New Age International.

Lindgren, P. (2016), GDPR regulation impact on different business models and businesses. *Journal of Multi Business Model Innovation and Technology*, 4(3), 241-254.

Οδηγία 201/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου του έτους 2016

Παναγοπούλου - Κουτνατζή, Φ., (2017) Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη

Ρόκας Ν./ Γκόρτσος Χ. / Μικρουλέα Α./ Λιβαδά Χ., (2016) Στοιχεία Τραπεζικού Δικαίου, Νομική Βιβλιοθήκη, 3η αναθεωρημένη έκδοση

Σωτηρόπουλος Β., (2019), Υπεύθυνος Προστασίας Δεδομένων, Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, Β΄ έκδοση

Τζιώρατζη, Β. (2018), Προστασία δεδομένων προσωπικού χαρακτήρα στον Χώρο Ελευθερίας, Ασφάλειας & Δικαιοσύνης, Νομική Βιβλιοθήκη

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018), EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153.

Wheatley, S., Maillart, T., & Sornette, D. (2016), The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, 89, 1-12.

Χριστοδούλου, Κ., (2020b) Δίκαιο προσωπικών δεδομένων: Γενικός κανονισμός 679 / 2016 GDPR - Εκτελεστικός νόμος 4624 / 2019 - Ν 3471 / 2006 για δημόσια ηλεκτρονικά δίκτυα, Νομική Βιβλιοθήκη, Αθήνα, σ. 174

Xuereb, K., Grima, S., Bezzina, F., Farrugia, A., & Marano, P. (2019), The impact of the general data protection regulation on the financial services' industry of small European states.

Ηλεκτρονικές πηγές

Άρθρο 4 – Γενικός Κανονισμός για την Προστασία δεδομένων – Ορισμοί
<https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-4-genikos-kanonismos-gia-tin-prostasia-dedomenon-orismoι> (Τελευταία επίσκεψη 07 Οκτωβρίου 2024)

GDPR – Εισαγωγή στο νέο Γενικό Κανονισμό Προστασίας Δεδομένων, Ανακτήθηκε από <https://www.gdprgreece.com/article/5/gdpr> (Τελευταία επίσκεψη 05 Οκτωβρίου 2024)

GDPR: Οδηγός Προστασίας Δεδομένων για Μικρές Επιχειρήσεις, Ανακτήθηκε από <https://www.taxheaven.gr/news/68213/gdpr-odhgios-prostasias-dedomenwn-gia-mikres-epixeirhseis> (Τελευταία επίσκεψη 01 Οκτωβρίου 2024)

Οδηγία για την ασφαλή καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας, Ανακτήθηκε από <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/odigia-gia-tin-asfali-katastrofi-prosopikon-dedomenon-meta-peras-tis> (Τελευταία επίσκεψη 05 Οκτωβρίου 2024)

ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002, Ανακτήθηκε από <https://www.dpa.gr/sites/default/files/2020-06/CELEX%2032002L0058%20EL%20TXT.pdf> (Τελευταία επίσκεψη 05 Οκτωβρίου 2024)

Protection of personal data, Ανακτήθηκε από <https://eur-lex.europa.eu/EL/legal-content/summary/protection-of-personal-data.html> (Τελευταία επίσκεψη 05 Οκτωβρίου 2024)

Τι είναι τα δεδομένα προσωπικού χαρακτήρα; Τι είναι τα δεδομένα προσωπικού χαρακτήρα; | Ευρωπαϊκή Επιτροπή, Ανακτήθηκε από www.europa.eu (Τελευταία επίσκεψη 30 Σεπτεμβρίου 2024)

Σημεία προσοχής για μικρές ή μεσαίες επιχειρήσεις, Ανακτήθηκε από https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/shmeia_prosoxhs_asfaleia_proswpikwn (Τελευταία επίσκεψη 05 Οκτωβρίου 2024)

