ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΕΛΕΓΚΤΙΚΗ

Διπλωματική Εργασία

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ ΣΤΑ ΠΛΑΙΣΙΑ ΤΟΥ GDPR: Η ΠΕΡΙΤΩΣΗ ΤΩΝ ΛΟΓΙΣΤΙΚΩΝ ΓΡΑΦΕΙΩΝ ΣΤΗ ΘΕΣΣΑΛΟΝΙΚΗ

της

ΘΕΟΔΩΡΙΔΟΥ ΘΑΛΕΙΑΣ

Επιβλέπων Καθηγητής: Λιβάνης Ευστράτιος

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στην Εφαρμοσμένη Λογιστική και Ελεγκτική

Οκτώβριος 2020

ΕΥΧΑΡΙΣΤΙΕΣ

Πρωτίστως, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Λιβάνη Ευστράτιο, για την πολύτιμη βοήθεια και καθοδήγηση που μου προσέφερε καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας.

Επίσης, ένα τεράστιο ευχαριστώ οφείλω στους γονείς μου, οι οποίοι με στηρίζουν σε κάθε μου βήμα όλα αυτά τα χρόνια, βοηθώντας με να κατακτήσω τους στόχους μου.

Τέλος, θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους τους καθηγητές του ΠΜΣ της Εφαρμοσμένη Λογιστικής και Ελεγκτικής για τις χρήσιμες γνώσεις που αποκόμισα.

ΠΕΡΙΛΗΨΗ

Η ραγδαία ανάπτυξη της τεχνολογίας ανά τα χρόνια αναγκάζει τις επιχειρήσεις να εναρμονιστούν με τις απαιτήσεις της ψηφιακής εποχής. Το γεγονός αυτό έχει οδηγήσει σε αυξημένη διασυνοριακή ροή πληροφοριών και ανταλλαγή μεγάλου όγκου προσωπικών δεδομένων, δημιουργώντας ζητήματα σχετικά με τους κινδύνους και την ασφάλεια των εταιριών στον κυβερνοχώρο. Στις 25 Μαΐου 2018, ο Γενικός Κανονισμός Προστασίας Δεδομένων αντικατέστησε την οδηγία 95/46/ΕΚ, αποσκοπώντας στην δημιουργία των κατάλληλων συνθηκών για την προστασία των ατομικών δικαιωμάτων στην ιδιωτικότητα.

Ο γενικός κανονισμός της ΕΕ για την προστασία των δεδομένων (GDPR) μπορεί να χαρακτηριστεί ως ένας από τους πλέον απαιτητικούς και ολοκληρωμένους κανονισμούς για την προστασία της ιδιωτικής ζωής όλων των εποχών. Δύο χρόνια αφότου τέθηκε σε υποχρεωτική εφαρμογή, μελετήσαμε τον αντίκτυπό του στο επάγγελμα των λογιστών και πιο συγκεκριμένα πραγματοποιήσαμε έρευνα σε λογιστικά γραφεία του νομού Θεσσαλονίκης.

Με βάση τα δεδομένα που συλλέχθηκαν, διαπιστώθηκε ότι το μεγαλύτερο ποσοστό των συμμετεχόντων είναι ενημερωμένο για την εφαρμογή του Κανονισμού και προσπαθεί να εναρμονιστεί πλήρως με τις απαιτήσεις του, λαμβάνοντας τα απαραίτητα μέτρα. Ωστόσο, η προσπάθεια φαίνεται πως δεν σταματάει εδώ, καθώς μέτρα όπως τα ασφαλιστήρια συμβόλαια έναντι των κινδύνων στον κυβερνοχώρο απαιτούν χρόνο προκειμένου να γίνουν ευρέως αποδεκτά από την ελληνική αγορά.

ABSTRACT

The rapid development of technology over the years has forced businesses to adapt to the demands of the digital age. This has led to an increased cross-border flow of information and an exchange of large amounts of personal data, creating issues about the risks and security of companies in cyberspace. On 25 May 2018, the General Data Protection Regulation replaced Data Protection Directive 95/46/EC, with the aim of creating the appropriate conditions for the protection of individual rights to privacy.

The EU's General Data Protection Regulation (GDPR) can be described as one of the most demanding and comprehensive privacy regulations of all time. Two years after it came into force, we studied its impact on the profession of accountant and, more specifically, we conducted a survey in the accountancy offices of the county of Thessaloniki.

Based on the the data collected in this research, it was found that the majority of participants are informed of the implementation of the GDPR and try to meet the corresponding requirements, by taking the necessary measures. However, the effort seems not to stop there, as measures such as cyber insurance contracts require time to be widely accepted by the Greek market.

“The GDPR is not anti-business;
there’s a lot of money to be made
by protecting people’s individual rights.”
-Karl Hennessee

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

Σελίδα

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Θεωρητικό υπόβαθρο

Μετά από χρόνια συζητήσεων, το GDPR τέθηκε σε ισχύ προκειμένου να αντικαταστήσει την οδηγία 95/46/ΕΚ για την προστασία των δεδομένων. Ο σχεδιασμός του αποσκοπεί στον εκσυγχρονισμό της νομοθεσίας περί απορρήτου των δεδομένων σε όλη την Ευρώπη, την προστασία της ιδιωτικής ζωής των πολιτών της ΕΕ και την αλλαγή του τρόπου με τον οποίο οι οργανισμοί προσεγγίζουν τα ζητήματα της προστασίας των πληροφοριών. Με άλλα λόγια, το GDPR θεσπίστηκε για να επιφέρει καινοτόμες αλλαγές στην ισχύουσα νομοθεσία.

Από το 2016, προτού ακόμη τεθεί σε εφαρμογή, ερευνητές από διαφορετικούς τομείς άρχισαν να αξιολογούν τον τρόπο με τον οποίο το GDPR θα επηρεάσει διάφορες δραστηριότητες, όπως το μάρκετινγκ και η τεχνολογία πληροφορικής. Ωστόσο, έχουν παρασχεθεί ελάχιστες πληροφορίες σχετικά με τον αντίκτυπο του κανονισμού όσον αφορά τις λογιστικές διαδικασίες.

Οι εν λόγω διαδικασίες είναι πολύπλοκες και χρησιμοποιούν σημαντικό όγκο προσωπικών δεδομένων. Στην πλειονότητα των περιπτώσεων, οι λογιστές χειρίζονται προσωπικά δεδομένα φυσικών προσώπων ή εργαζομένων, όπως αρχεία μισθοδοσίας και κοινωνικών εισφορών, δεδομένα πελατών κ.α. Παρ' όλα αυτά, λόγω έλλειψης καλής κατανόησης των κύριων μέτρων ασφάλειας των πληροφοριών, εντοπίζεται δυσκολία επιλογής και εφαρμογής των βέλτιστων πρακτικών ώστε να συμμορφώνονται με το GDPR, επιτυγχάνοντας την πρόληψη των παραβιάσεων των δεδομένων. Ως εκ τούτου, η κατάρτιση των λογιστών για τη διαχείριση και την αντιμετώπιση των διαρροών δεδομένων αποτελεί σημαντικό βήμα για την υιοθέτηση των κανόνων του GDPR. Επομένως, κρίνεται απαραίτητο για τους λογιστές να αυξήσουν το επίπεδο ευαισθητοποίησης και τις ικανότητές τους να προστατεύουν κάθε είδος ευαίσθητων ή προσωπικών δεδομένων καθώς σε διαφορετική

περίπτωση ελλοχεύει ο κίνδυνος να μην επιτευχθεί πλήρως η συμμόρφωση με το Γενικό Κανονισμό.

Έρευνα με σχετική θεματολογία διεξήχθη στη Ρουμανία, μέσω αποστολής ερωτηματολογίου σε 200 λογιστές, οικονομικούς και εσωτερικούς ελεγκτές που εργάζονται σε ρουμανικές επιχειρήσεις προκειμένου να αξιολογηθεί ο αντίκτυπος του γενικού κανονισμού για την προστασία των δεδομένων στην περίπτωση των λογιστικών υπηρεσιών. Τα αποτελέσματα υπογράμμισαν σαφώς ένα κενό γνώσης μεταξύ της πραγματικής πρακτικής και των προσδοκιών. Επιπλέον, μετά την ανάλυση των ακολουθούμενων διαδικασιών των λογιστών προκειμένου να διασφαλίσουν τις δραστηριότητές τους, έχει επισημανθεί το γεγονός ότι μπορεί να μην κατανοούν πλήρως τα μέσα προστασίας των προσωπικών και ιδιωτικών πληροφοριών. Ωστόσο, η μελέτη αυτή διεξήχθη μερικούς μήνες πριν την καθολική εφαρμογή του Γενικού Κανονισμού, γεγονός που κάνει τους συγγραφείς να αναμένουν μείωση αυτού του χάσματος γνώσης στο εγγύς μέλλον (Stanciu & Rîndaşu, 2018).

1.2 Σκοπός της εργασίας

Σκοπός της παρούσας διπλωματικής είναι να διερευνηθεί κατά πόσο τα λογιστικά γραφεία γνωρίζουν και εφαρμόζουν τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων που τέθηκε σε εφαρμογή τον Μάϊο του 2018. Επιπλέον, αντικείμενο μελέτης αποτέλεσαν και τα μέτρα τα οποία έχουν λάβει προκειμένου επιτευχθεί αυτό.

1.3 Ερευνητικά ερωτήματα

Τα ερευνητικά ερωτήματα που τέθηκαν είναι τα εξής:

1. Εάν τα λογιστικά γραφεία γνωρίζουν το νέο Ευρωπαϊκό Κανονισμό (5419/16), που αφορά την προστασία προσωπικών δεδομένων
2. Εάν έχουν λάβει μέτρα προκειμένου να συμμορφωθούν με τις απαιτήσεις του Κανονισμού
3. Εάν νιώθουν ευάλωτοι απέναντι σε κινδύνους απώλειας ή διαρροής δεδομένων λόγω των υπηρεσιών cloud που χρησιμοποιούν

4. Εάν επιλέγουν τα ασφαλιστήρια συμβόλαια ως μέτρο αντιμετώπισης των διαδικτυακών κινδύνων.

1.4 Μεθοδολογία

Επιλέχθηκε η μέθοδος της ποσοτικής έρευνας με ερωτηματολόγιο. Το δείγμα της έρευνας αποτέλεσαν 89 λογιστικά γραφεία του νομού Θεσσαλονίκης τα οποία συλλέχθηκαν μέσω ιστοσελίδων που παρέχουν υπηρεσίες εύρεσης πληροφοριών. Το ποσοστό συμμετοχής στην έρευνα είναι 38,2% καθώς λάβαμε απαντήσεις από τα 34 εξ' αυτών.

1.5 Δομή εργασίας

Η διπλωματική εργασία χωρίζεται σε δύο μέρη. Στο πρώτο κομμάτι γίνεται αναλυτική παράθεση των βιβλιογραφικών πηγών που σχετίζονται με το θέμα, ενώ στο δεύτερο μέρος παρουσιάζονται τα αποτελέσματα της ποσοτικής έρευνας που πραγματοποιήθηκε.

Αναλυτικότερα, η εργασία αποτελείται από επτά Κεφάλαια. Το δεύτερο κεφάλαιο απαρτίζουν κομμάτια της παγκόσμιας βιβλιογραφίας και επιστημονικής αρθρογραφίας σχετικά με την εφαρμογή του Γενικού Κανονισμού, τους κινδύνους και την ασφάλεια στον κυβερνοχώρο.

Στο τρίτο Κεφάλαιο δίνεται περισσότερη βαρύτητα στην έννοια του κινδύνου στον κυβερνοχώρο και παρουσιάζονται οι επιμέρους κατηγορίες των κινδύνων αυτών. Επιπρόσθετα, αναλύονται οι κατηγορίες που διακρίνονται οι επίδοξοι χάκερ, καθώς επίσης και τα μέτρα προστασίας που μπορούν να λάβουν οι επιχειρήσεις προκειμένου να αποτρέψουν τα πιθανά συμβάντα που θα προκύψουν σε σχέση με τον κίνδυνο στον κυβερνοχώρο.

Στο τέταρτο Κεφάλαιο αναλύεται ο νέος Ευρωπαϊκός Κανονισμός και παρουσιάζονται οι βασικότερες αρχές που τον διέπουν. Επιπλέον, γίνεται αναφορά στα πρόστιμα-ποινές που ορίζονται μέσα στο κείμενο του GDPR, παραθέτοντας τα μεγαλύτερα ποσά προστίμων που έχουν καταγραφεί μέσα στο προηγούμενο έτος.

Το δεύτερο μέρος της διπλωματικής που σχετίζεται με το ερευνητικό κομμάτι, ξεκινάει από το πέμπτο κεφάλαιο, όπου γίνεται μια παρουσίαση της μεθοδολογίας που ακολουθήθηκε και συνεχίζεται στο έκτο κεφάλαιο με την ανάλυση των αποτελεσμάτων που προέκυψαν.

Η εργασία ολοκληρώνεται με το έβδομο κεφάλαιο που περιέχει τα συμπεράσματα και τις προτάσεις για περαιτέρω ερεύνα.

1.6 Συνεισφορά στη βιβλιογραφία

Η συνεισφορά στη βιβλιογραφία είναι πολλαπλή καθώς το GDPR και οι επιπτώσεις αυτού στον επιχειρηματικό κλάδο αποτελούν ένα ζήτημα σχετικά νέο στον ερευνητικό κόσμο, καθώς έχουν περάσει μόλις δύο έτη από την καθολική εφαρμογή του στις χώρες της Ευρωπαϊκής Ένωσης. Συνεπώς, οποιαδήποτε ερευνητική προσπάθεια αποτελεί ένα ακόμη εργαλείο ερμηνείας των αλλαγών που έχει επιφέρει από την έναρξη της εφαρμογής του μέχρι και σήμερα.

ΚΕΦΑΛΑΙΟ 2

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Εισαγωγή

Στο παρόν κεφάλαιο παραθέτουμε πληροφορίες από την παγκόσμια βιβλιογραφία και αρθρογραφία σχετικά με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων, τους κινδύνους και την ασφάλεια στον Κυβερνοχώρο.

2.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Η δημοσίευση άρθρων σχετικών με το GDPR ξεκίνησε ήδη από το 2016, πριν ακόμη δημοσιευθεί το πλήρες κείμενο του κανονισμού, καθώς αποτέλεσε θέμα υψίστης σημασίας για όλες τις επιχειρήσεις εξαιτίας της καθολικότητας της εφαρμογής του. Ένα βασικό ζήτημα που απασχόλησε μεγάλο ποσοστό των επιστημόνων που αποφάσισαν να ασχοληθούν τα πρώτα χρόνια με το θέμα είναι οι αλλαγές που θα επιφέρει το GDPR στον επιχειρηματικό κόσμο. Αυτό που επισημαίνεται, κυρίως, είναι ότι δεν υπήρχε αρκετός χρόνος έως την επίσημη εφαρμογή του Γενικού Κανονισμού ώστε, τόσο οι επιχειρήσεις, δικηγορικές και συμβουλευτικές εταιρείες όσο και οι πάροχοι ηλεκτρονικών υπηρεσιών να προλάβουν να εναρμονιστούν με τις απαιτήσεις του GDPR. Επίσης, λόγω της αυξημένης πολυπλοκότητάς του δεν ήταν εύκολο να σχηματίσουν μια καθαρή εικόνα των προκλήσεων που έχουν να αντιμετωπίσουν στην συνέχεια. Βέβαια, χαρακτηρίζεται ως θετικό το γεγονός ότι αποτελεί έναν ενιαίο κανονισμό καθώς καθιστά εφικτή την γρηγορότερη ενσωμάτωση και υιοθέτησή του από τις αρχές και τα κράτη της Ε.Ε. Ένα ακόμη θετικό στοιχείο το οποίο αναφέρουν οι ερευνητές είναι ότι με την άμεση ταυτοποίηση των χρηστών μειώνεται κατά πολύ η άσκοπη

ανταλλαγή προσωπικών δεδομένων. Συνεπώς, εξαλείφεται η πιθανότητα απώλειας των δεδομένων αυτών (Ryz , et al., 2016).

Η αποτελεσματικότητα του νέου Κανονισμού για την προστασία των προσωπικών δεδομένων εξετάστηκε, επίσης, από πολλούς καθώς αποτελεί θέμα υπό αμφισβήτηση. Μέσω της σύγκρισης, κυρίως, των προηγούμενων κειμένων επί του θέματος, γίνεται αντιληπτό το γεγονός ότι η εφαρμογή του νέου αυτού Κανονισμού αποτελεί σημαντικό βήμα για την προστασία των προσωπικών δεδομένων. Πιο συγκεκριμένα, οι συγγραφείς θεωρούν ότι, παρά τις τροποποιήσεις που έχουν γίνει στο βασικό κείμενο, έχοντας προκαλέσει σημαντικές αμφιβολίες, ο σκοπός του κειμένου δεν έχει αλλάξει. Συνεπώς, συμφωνούν με την θέσπισή του και επικροτούν τα θετικά αποτελέσματα που θα έχει παγκοσμίως. Παρ' όλα αυτά οι επιστήμονες πιστεύουν ότι το κλειδί για την επιτυχία είναι η συνεχής ενημέρωση και επαγρύπνηση των αρχών προκειμένου να αντιμετωπιστούν τυχόν αμβλώσεις στη συνέχεια (De Hert & Papakonstantinou, 2016).

Φυσικά, υπήρξαν διάφοροι υποστηρικτές του Κανονισμού, οι οποίοι σε σχετικά τους άρθρα παραθέτουν, εν συντομία, τα οφέλη που δημιουργεί η εφαρμογή και προώθηση αυτού. Σύμφωνα με τους ίδιους, ο Κανονισμός επιλύει διάφορα ζητήματα που χρήζουν αντιμετώπισης εδώ και πολλά χρόνια. Ο σχεδιασμός του GDPR έγινε με γνώμονα την ασφάλεια αλλά και την εξασφάλιση των προσωπικών δεδομένων, ωθώντας τις επιχειρήσεις να αναπροσαρμόσουν τα συστήματά τους προκειμένου να ελαχιστοποιήσουν τις παραβάσεις και τις απώλειες τέτοιων δεδομένων. Αυτό οδηγεί τις επιχειρήσεις σε ένα συνεχώς αναπτυσσόμενο ψηφιακό μέλλον με το οποίο θα πρέπει να συμβαδίζουν τα επόμενα χρόνια. Είναι δεδομένο, δυστυχώς, ότι δεν θα πάψουν να υφίστανται οι επιθέσεις στον κυβερνοχώρο. Για το λόγο αυτό, είναι χρέος των εταιριών να αποκτήσουν τα κατάλληλα εφόδια ώστε να τις αντιμετωπίσουν, έχοντας πάντα την ελάχιστη δυνατή απώλεια προσωπικών δεδομένων, διότι είναι δική τους ευθύνη να εξομαλύνουν τις συνέπειες από μία τέτοια επίθεση προστατεύοντας τα δεδομένα των χρηστών από κάθε κίνδυνο (Zerlang, 2017).

Οι απαραίτητες ενέργειες από πλευράς επιχειρήσεων ώστε να επιτύχουν την ομαλότερη εναρμόνιση με τις απαιτήσεις του νέου Κανονισμού αποτέλεσαν, λοιπόν, αντικείμενο μελέτης αρκετών ερευνητών. Στα πλαίσια αυτής, εντοπίστηκαν οι σημαντικότερες ενέργειες που οφείλουν να ακολουθήσουν οι επιχειρήσεις προκειμένου να είναι σύμφωνες με τα πρότυπα του GDPR. Αυτές είναι οι εξής: α) να παρέχουν το δικαίωμα στη λήθη σε όποιον το επιθυμεί, β) να μπορεί ο ενδιαφερόμενος να δώσει μια σαφή και ρητή

συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων, γ) να δίνουν το δικαίωμα της ασφαλής και γρήγορης μεταφοράς των δεδομένων από τον έναν πάροχο υπηρεσιών στον άλλον, δ) να ορίζουν υπεύθυνο επεξεργασίας δεδομένων, με σκοπό να έχει επαφή με οποιαδήποτε εποπτική αρχή, αν παρουσιαστεί οποιοδήποτε πρόβλημα και ε) να διασφαλίζουν ότι η επεξεργασία δεδομένων πραγματοποιείται μέσω τεκμηριωμένων διαδικασιών, είτε από την ίδια την επιχείρηση είτε από τρίτους που την διενεργούν για λογαριασμό της. Κάθε σχετικό έγγραφο θα πρέπει να είναι διαθέσιμο κατά την διάρκεια ενός ελέγχου (Krystlik, 2017).

Πέρα απ' όλες τις προκλήσεις που πρέπει να αντιμετωπίσουν οι οργανισμοί, το δικαίωμα στη λήθη, δηλαδή το δικαίωμα διαγραφής από τα αντίγραφα ασφαλείας και τα αρχεία αποτελεί ακανθώδες ζήτημα γι' αυτές. Όπως επισημαίνεται σε σχετικό άρθρο, οι υπεύθυνοι επεξεργασίας έχουν υποχρέωση να διαγράψουν οποιαδήποτε πληροφορία ζητήσει το υποκείμενο των δεδομένων οποιαδήποτε στιγμή. Το γεγονός αυτό επηρεάζει σε μεγάλο βαθμό τις διαδικασίες διατήρησης δεδομένων και δημιουργίας αντιγράφων ασφαλείας. Ως εκ τούτου, στο κομμάτι της μακροχρόνιας αρχειοθέτησης, δημιουργούνται ζητήματα εντός των οργανισμών σχετικά με τον εντοπισμό και την χρήση προσωπικών πληροφοριών για τα οποία έχουν δημιουργηθεί αντίγραφα ασφαλείας ή έχουν αρχειοθετηθεί, ή χρησιμοποιούνται στην προηγμένη ανάλυση δεδομένων των ERP συστημάτων. Συμπερασματικά, προκύπτουν σοβαρές επιπτώσεις τόσο για τα πρότυπα δημιουργίας αντιγράφων ασφαλείας, όσο και για τις υπηρεσίες αναζήτησης και ευρετηρίου, τα οποία πρέπει αναπόφευκτα να ευθυγραμμιστούν με τις διατάξεις του GDPR (Politou, et al., 2018).

Επιπρόσθετα, διερευνήθηκαν οι πρακτικές επιπτώσεις του Κανονισμού εξαιτίας των οργανωτικών και τεχνικών μέτρων που έλαβαν οι εταιρίες, οι οποίες χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα, καθότι επηρεάστηκε η στρατηγική και η πολιτικής τους. Η κατανόηση αυτών των επιπτώσεων έχει ουσιαστική σημασία για τις επιχειρήσεις, καθώς απαιτούνται σημαντικά χρονικά διαστήματα, στρατηγικός σχεδιασμός, εκπαίδευση των εργαζομένων, οικονομικοί και ανθρώπινοι πόροι για την εφαρμογή των απαιτήσεων του GDPR. Οι εν λόγω επιπτώσεις που έχει επιφέρει η εφαρμογή του Κανονισμού ταξινομήθηκαν εντός ενός πλαισίου 12 πτυχών, οι οποίες περιλαμβάνουν επίσης, τα κατάλληλα μέτρα και την επιχειρηματική στρατηγική που οφείλουν να ακολουθήσουν οι επιχειρήσεις. Τέλος, είναι ωφέλιμο για τις εταιρίες να αξιοποιήσουν και τις υπάρχουσες κατευθυντήριες γραμμές προκειμένου να επιτύχουν μια αποτελεσματική προετοιμασία (Tikkinen-Piri, et al., 2018).

Με βάση τα παραπάνω, συμπεραίνουμε ότι το GDPR θα μπορούσε να θεωρηθεί από τους οργανισμούς υπερβολικά απαιτητικό. Παρ' όλα αυτά, όμως, η συντριπτική πλειοψηφία αισθάνεται ότι ο Κανονισμός δεν είναι αρκετά περιοριστικός, καθώς δίνει κατευθύνσεις για το τι πρέπει να κάνουν οι εταιρίες αλλά δεν διευκρινίζει το πώς να το κάνουν. Η πραγματική πρόκληση για τις επιχειρήσεις είναι να πάρουν εκατοντάδες σελίδες νομικής ορολογίας και να βρουν πως να τις αντιστοιχίσουν με την κατάλληλη τεχνολογία ώστε να επιτύχουν την πλήρη συμμόρφωση με το GDPR. Η διαδικασία αυτή για πολλούς μπορεί να είναι χρονοβόρα. Επομένως, προτείνεται να περατωθεί από ειδικούς συνεργάτες που γνωρίζουν καλά τον Κανονισμό και μπορούν με συγκεκριμένες μεθόδους να καταρτίσουν τον κατάλληλο οδηγό συμμόρφωσης για την κάθε περίπτωση (Garber & Focus, 2018).

Δυστυχώς, δεν υπάρχει τρόπος προκειμένου αυτές οι διαδικασίες να γίνουν άμεσα και αποτελεσματικά. Σε σχετική έρευνα που πραγματοποιήθηκε στην Αμερική το 2018, διαπιστώθηκε ότι υπήρξε μια αξιοσημείωτη έλλειψη ενημέρωσης για τον Γενικό Κανονισμό από την πλευρά των επιχειρήσεων. Επίσης, από πολλούς το GDPR θεωρήθηκε ως ευρωπαϊκός νόμος που ισχύει μόνο για την ΕΕ και όχι για τις ΗΠΑ ή τις υπόλοιπες χώρες. Παράλληλα, στην ίδια έρευνα εκτιμήθηκε ότι οι μισές από τις εταιρείες που διαχειρίζονται προσωπικά δεδομένα δεν θα έχουν συμμορφωθεί πλήρως μέχρι το τέλος του 2018. Με άλλα λόγια, ακόμη και αν οι νομικές τους ομάδες και οι ομάδες ασφαλείας συγκεντρώσουν τις δυνάμεις τους για να προετοιμαστούν για το GDPR, υπάρχουν τμήματα όπως το οικονομικό, το μάρκετινγκ και άλλα που πιθανόν να καθυστερούν (Miglicco, 2018).

Ένα ακόμη περιστατικό που σχετίζεται με τις ΗΠΑ και πιο συγκεκριμένα με τις εταιρίες Chicago Times και LA Times έλαβε χώρα το 2018. Οι εν λόγω εταιρείες εδρεύουν στην Αμερική και παρέχουν υπηρεσίες ηλεκτρονικής και έντυπης ενημέρωσης. Δεδομένου ότι δεν πληρούσαν τις προδιαγραφές του GDPR αποφάσισαν να σταματήσουν την είσοδο στις υπηρεσίες τους για τους ευρωπαίους πελάτες, φοβούμενες τις υψηλές κυρώσεις σε περίπτωση καταγγελίας. Με τον τρόπο αυτό, θεώρησαν ότι έπαψαν να είναι υπόλογες προς τους κανονισμούς που θέτει το GDPR. Η συγκεκριμένη πρακτική είναι εσφαλμένη και μόνο αρνητικές συνέπειες θα μπορούσε να έχει (Datoo, 2018).

Σε άλλη έρευνα σχετική με το GDPR και την ιατρική επιστήμη, μέσω προσωπικών συνεντεύξεων με στελέχη γνωστών ιατρικών εταιριών παρατηρήθηκε ότι υπάρχει προβληματισμός σε σχέση με την εφαρμογή του Κανονισμού στο συγκεκριμένο κλάδο. Αυτό συμβαίνει κυρίως σε περιπτώσεις όπου, οι ασθενείς δεν επιθυμούν να δώσουν την

συγκατάθεσή τους για επεξεργασία των προσωπικών τους δεδομένων ενώ είναι απαραίτητο για τη διασφάλιση της δημόσιας υγείας. Συνεπώς, είναι πιθανό να δημιουργούνται θέματα αντιπαράθεσης του Γενικού Κανονισμού με την ισχύουσα νομοθεσία (McCall, 2018).

Ερευνώντας τα οφέλη της συμμόρφωσης με το GDPR, εντοπίστηκαν ορισμένα από αυτά, όπως, η ορθή διαχείριση των δεδομένων, η αύξηση της διαφάνειας, της φήμης καθώς επίσης και της ανταγωνιστικότητας. Σε αντίθεση με αυτά όμως υπάρχουν και αρκετά εμπόδια όσον αφορά την εφαρμογή του Κανονισμού. Το κυριότερο από αυτά πηγάζει από το ίδιο το κείμενο του Κανονισμού καθώς οι ερευνητές το χαρακτηρίζουν πολύπλοκο, εκτεταμένο και σε πολλά σημεία του απαιτεί υποκειμενικότητα. Η έλλειψη γνώσεων και εμπειρίας σχετικά με την προστασία της ιδιωτικής ζωής, η απαιτούμενη τεχνολογία και οι πρακτικοί οδηγοί ή οι τυποποιημένες διαδικασίες αποτελούν, επίσης, σημαντικά εμπόδια. Επομένως, κρίνεται απαραίτητη η θέσπιση μέτρων προστασίας προκειμένου να επιτευχθεί η σωστή υλοποίηση του GDPR. Για παράδειγμα, η ανάλυση των απαιτήσεών του, ο προσδιορισμός των κινδύνων, η τεκμηρίωση των εργασιών επεξεργασίας, η εφαρμογή σωστής διαχείρισης δεδομένων και ο ορισμός υπεύθυνου προστασίας (DPO) αποτελούν βασικούς πυλώνες για την ορθή εφαρμογή του Κανονισμού (Teixeira, et al., 2019).

Τέλος, πολλοί χαρακτηρίζουν το GDPR ως ένα νέο παράδειγμα στη διαδικασία χειραγώγησης και διαχείρισης των προσωπικών δεδομένων. Οι εταιρείες είναι αυτές που έχουν πλέον την ευθύνη να εγκρίνουν μέτρα ελέγχου, παρακολούθησης και λογιστικού ελέγχου. Λόγω αυτού, το GDPR έχει επιφέρει νομικές, τεχνικές και οργανωτικές αλλαγές στις εταιρείες που δραστηριοποιούνται στην πληροφορική και έχει συμβάλλει σε μια παραδειγματική αλλαγή της στρατηγικής των οργανισμών. Σε αντίστοιχη μελέτη, διαπιστώθηκε ότι τα οφέλη και οι προκλήσεις που αντιμετωπίζουν οι εταιρείες πληροφορικής ποικίλουν με βάση το μέγεθος τους. Πιο συγκεκριμένα, οι μεγαλύτερες επιχειρήσεις εμφάνισαν μεγαλύτερη αντίληψη των θετικών επιπτώσεων όπως η εμπιστοσύνη, η ελαχιστοποίηση της ανάγκης για προσωπικά δεδομένα, η βελτίωση των διαδικασιών διαχείρισης και η δημιουργία νέων ανταγωνιστικών πλεονεκτημάτων. Βέβαια, εντοπίστηκε δυσκολία στην εφαρμογή του δικαιώματος της διαγραφής των προσωπικών δεδομένων, ή αλλιώς του δικαιώματος στη λήθη που αποτελεί ένα από τα βασικότερα δικαιώματα που θεσμοθετήθηκε με την εφαρμογή του GDPR. Από την άλλη μεριά, οι μικρότερες επιχειρήσεις είχαν μεγαλύτερη αντίληψη των προκλήσεων που σχετίζονται με την αύξηση της τεχνικής πολυπλοκότητας και την ανάγκη ανάπτυξης νέων τεχνολογιών (Poritskiy, et al., 2019).

2.3 Ο Κυβερνοχώρος

2.3.1 Εισαγωγή

Υπάρχουν πολλά παραδείγματα της υψηλής οικονομικής και κοινωνικής σημασίας του κινδύνου στον κυβερνοχώρο. Κάθε αναφερόμενο συμβάν παραβίασης δεδομένων ή βλάβης του συστήματος ασφαλείας που έχει ως αποτέλεσμα οικονομική ζημία ή απώλεια φήμης αυξάνει την επίγνωση των υπεύθυνων λήψης αποφάσεων ότι τα ισχύοντα ασφαλιστήρια συμβόλαια δεν καλύπτουν επαρκώς τους κινδύνους στον κυβερνοχώρο.. Η ασφάλιση θεωρείται μια δυνατότητα για τη διαχείριση της έκθεσης σε κίνδυνο στον κυβερνοχώρο. Παρά την αυξανόμενη σημασία της για τις επιχειρήσεις σήμερα, η έρευνα για τον κίνδυνο στον κυβερνοχώρο είναι αρκετά περιορισμένη. Στον τομέα της τεχνολογίας υπάρχουν σχετικές μελέτες, ενώ στον τομέα των κινδύνων και των ασφαλίσεων είναι αισθητά λιγότερες (Biener, et al., 2015).

2.3.2 Οι κίνδυνοι του Κυβερνοχώρου (cyber risk)

Η χρήση του Διαδικτύου έχει αυξήσει σημαντικά την ευπάθεια των οργανισμών στις επιθέσεις κλοπής και απώλειας δεδομένων, φέρνοντας έτσι τα θέματα ασφαλείας των πληροφοριών στην πρώτη γραμμή της ημερήσιας διάταξης για τα εταιρικά στελέχη. Η σημασία αυτού του θέματος επισημαίνεται σε μια έρευνα του 2002 που διεξήχθη από το Ινστιτούτο Ασφάλειας των Υπολογιστών και το Ομοσπονδιακό Γραφείο Ερευνών. Η έρευνα του CSI/FBI ανέφερε ότι το 90% των ερωτηθέντων εντόπισε παραβίαση της ασφάλειας του υπολογιστή το προηγούμενο έτος και η μέση εκτιμώμενη ζημία ήταν πάνω από 2 εκατομμύρια δολάρια ανά οργανισμό. Επιπλέον, το 74% των ερωτηθέντων ανέφερε ότι οι συνδέσεις τους στο Διαδίκτυο ήταν τα σημεία συχνών επιθέσεων (Power, 2002).

Οι οργανισμοί ασχολούνται εδώ και καιρό με την προστασία των πληροφοριών που τους αφορούν, τη διατήρηση της ακεραιότητας των βάσεων δεδομένων τους και τη διασφάλιση της πρόσβασης στις πληροφορίες από εξουσιοδοτημένους χρήστες. Ωστόσο, λόγω αυξημένης ευπάθειας σε σημαντικές οικονομικές ζημίες από επιθέσεις μέσω του

Διαδικτύου, πολλά στελέχη αναζητούν πρόσθετα εργαλεία για τη διαχείριση του κινδύνου ασφάλειας των πληροφοριών. Ένα νέο εργαλείο είναι η χρήση ασφαλιστηρίων συμβολαίων που παρέχουν κάλυψη έναντι ζημιών από παραβιάσεις στο Διαδίκτυο σχετικές με την ασφάλεια των πληροφοριών. Μέσω αυτής, μια επιχείρηση μπορεί να αντισταθμίσει τις πιθανές απώλειές της από το ηλεκτρονικό έγκλημα (Gordon, et al., 2003).

Μεγάλο μέρος του πιθανού κινδύνου από τη διεξαγωγή επιχειρηματικών δραστηριοτήτων στο Διαδίκτυο δεν είναι νέο. Για παράδειγμα, μια επιχείρηση θα διατρέχει κίνδυνο να υποστεί προσβολή των δικαιωμάτων πνευματικής ιδιοκτησίας ή δυσφήμηση είτε οι πληροφορίες διανέμονται μέσω του Διαδικτύου είτε μέσω τηλεόρασης, ραδιοφώνου ή περιοδικών. Παρομοίως, μια εταιρεία θα μπορούσε να υποστεί απώλεια επιχειρηματικής δραστηριότητας είτε από πυρκαγιά ή πλημμύρα, είτε από επίθεση άρνησης υπηρεσιών (denial of service attack) ενός χάκερ (Gordon, et al., 2003).

Είναι, λοιπόν, φανερό ότι ο κίνδυνος στον κυβερνοχώρο αποτελεί μια διαρκώς αυξανόμενη απειλή τόσο για τους δημόσιους όσο και για τους ιδιωτικούς οργανισμούς, λόγω των δυνητικά καταστροφικών επιπτώσεών του στα συστήματα πληροφοριών, τον κίνδυνο φήμης και την πιθανή απώλεια της εμπιστοσύνης των καταναλωτών. Με την έλευση του Διαδικτύου και την αντίστοιχη διάδοση της τεχνολογίας των πληροφοριών, οι επιχειρήσεις ήταν γενικά απροετοίμαστες για τον εντοπισμό και την αντιμετώπιση αυτού του κινδύνου. Επίσης, με την πάροδο του χρόνου η φύση των επιθέσεων έχει αλλάξει, καθώς έχουν αυξηθεί τόσο σε συχνότητα όσο και σε σοβαρότητα. Σε πολλές περιπτώσεις, οι δράστες επιθέσεων στον κυβερνοχώρο διέκοψαν τις επιχειρηματικές δραστηριότητες απλά για τη δική τους ψυχαγωγία, ή θεώρησαν την παραβίαση της υποδομής της τεχνολογίας της πληροφορίας ως πρόκληση (Brockett, et al., 2012).

Από τους πρώτους (ήπιους) χάκερ που εισέβαλαν σε συστήματα για να επιδείξουν τις ικανότητές τους, κάποιοι κατάφεραν να κερδίσουν χρήματα στο πλαίσιο εκμετάλλευσης μιας αναπτυσσόμενης επιχείρησης που αγνοούσε την ανασφάλεια του Διαδικτύου. Σε σύγκριση με τις επιθέσεις που είχαν ως αποτέλεσμα τη διακοπή του δικτύου σε μεγάλη κλίμακα, οι περισσότερες ηλεκτρονικές επιθέσεις σήμερα εξάγουν πολύτιμα δεδομένα, ενώ παραμένουν αρκετά κερδοφόρες για τους δράστες. Ένας από τους τύπους δεδομένων που στοχεύουν οι χακερ είναι οι προσωπικές πληροφορίες ταυτότητας (ID), όπως οι αριθμοί πιστωτικών καρτών, οι αριθμοί κοινωνικής ασφάλισης, οι τραπεζικοί λογαριασμοί και τα ιατρικά αρχεία. Δεδομένου ότι κάθε κλοπή ή διαρροή τέτοιων προσωπικών στοιχείων αποτελεί "απώλεια

ελέγχου" των ατομικών ιδιωτικών δεδομένων κάποιου, μπορεί να θεωρηθεί ήδη ως ζημιογόνο γεγονός, χωρίς να υπολογίζονται οι πιθανές πραγματοποιθείσες οικονομικές και κοινωνικές ζημίες. Στην πραγματικότητα, η κλοπή αναγνωριστικών δεδομένων είναι ο στόχος που είναι κοινός σε ένα ευρύ φάσμα μη καταστροφικών επιθέσεων στο Διαδίκτυο που εστιάζουν στο κέρδος. Η (ανεξέλεγκτη) διάδοση των προσωπικών πληροφοριών θέτει σε κίνδυνο τους ανθρώπους στην εποχή της τεχνολογίας των πληροφοριών (Maillart & Sornette, 2010).

Πέρα από τα φυσικά πρόσωπα, εξίσου συχνές είναι οι κυβερνοεπιθέσεις σε επιχειρήσεις καθώς οι περισσότερες δεν δίνουν την πρέπουσα σημασία προκειμένου να προστατευτούν έναντι των κινδύνων του κυβερνοχώρου. Έρευνες έχουν δείξει ότι αρκετές από αυτές διαθέτουν ελλιπή συστήματα ελέγχου και αξιολόγησης του κινδύνου καθώς και ανύπαρκτα μέτρα αντιμετώπισης αυτού. Επιπλέον, στον επιχειρηματικό τομέα, η ασφάλεια στον κυβερνοχώρο θεωρείται κυρίως αρμοδιότητα του τμήματος IT. Παρά το γεγονός ότι οι επαγγελματίες της πληροφορικής έχουν την δυνατότητα να κατανοούν και αντιμετωπίζουν θέματα σχετικά με την ασφάλεια στον κυβερνοχώρο, είναι πιθανόν να μην διαθέτουν τις απαραίτητες δεξιότητες για να εκπαιδεύσουν τους υπόλοιπους εργαζόμενους της εταιρίας. Τέλος, πολλές φορές η διοίκηση δεν διαθέτει τον απαραίτητο χρόνο προκειμένου να σχεδιάσει τα κατάλληλα μέτρα για την ασφάλεια στον κυβερνοχώρο καθώς δεν το θεωρεί πρόβλημα μείζονος σημασίας (Hall, 2016).

Η αποτελεσματική λήψη στρατηγικών αποφάσεων σχετικά με την επένδυση σε ασφαλιστικά πακέτα για την προστασία στον κυβερνοχώρο μελετήθηκε από αρκετούς ερευνητές. Ο βασικότερός τους στόχος ήταν να επισημάνουν τις αδυναμίες και τα πλεονεκτήματα των διαφορετικών επενδυτικών μεθόδων, το όφελος της αλληλεπίδρασής τους και τον αντίκτυπο που έχουν οι έμμεσες δαπάνες στις επενδύσεις για την ασφάλεια στον κυβερνοχώρο. Αξίζει να σημειωθεί ότι το εργαλείο που χρησιμοποιήθηκε σε αντίστοιχη μελέτη προκειμένου να υποστηρίξει τη λήψη στρατηγικών αποφάσεων σχετικών με τις επενδύσεις αυτές παρέχει τις ίδιες συμβουλές με αυτές που υποστηρίζει η κυβέρνηση του Ηνωμένου Βασιλείου για βασική προστασία από επιθέσεις στον κυβερνοχώρο (Fielder, et al., 2016).

Δυστυχώς, δεν είναι δυνατόν να εξαλειφθεί πλήρως ο κίνδυνος επίθεσης στον κυβερνοχώρο. Οι χάκερ θα συνεχίσουν να αναπτύσσουν νέες και εξεζητημένες μεθόδους για να παρακάμψουν ακόμα και την παραμικρή ασφάλεια. Ως εκ τούτου, θα πρέπει να καταρτιστεί σχέδιο ανάκαμψης το οποίο θα διασφαλίσει ότι μια επιχείρηση είναι ανθεκτική

και μια ανθεκτική επιχείρηση θα έχει ανταγωνιστικό πλεονέκτημα έναντι των μη ανθεκτικών ανταγωνιστών της. Επιπρόσθετα, οι οργανισμοί θα πρέπει να συνεργάζονται με έναν ασφαλιστή ο οποίος κατανοεί τους κινδύνους στον κυβερνοχώρο που αντιμετωπίζουν, όχι μόνο προσφέροντας πρακτικές συμβουλές πρόληψης, αλλά και ικανό να ανταποκριθεί σε περίπτωση επίθεσης (McKenna, 2018).

Είναι δεδομένο, πλέον, ότι η ασφάλεια στον κυβερνοχώρο αποτελεί στρατηγική επιχειρηματική προτεραιότητα, την οποία κανένας CEO δεν έχει την πολυτέλεια να αγνοήσει. Η ζημία που προκαλείται από την παραβίαση δεδομένων υπερβαίνει κατά πολύ το κόστος επιβολής προστίμων από τις αρχές. Το κόστος αυτό είναι δύσκολο να ποσοτικοποιηθεί. Έρευνες έδειξαν ότι οι σοβαρές παραβιάσεις μπορεί να έχουν τεράστιο αντίκτυπο στην τιμή των μετοχών μιας εταιρείας. Αυτό οφείλεται σε μεγάλο βαθμό στο γεγονός ότι, μετά από μια παραβίαση δεδομένων, κλονίζεται η εμπιστοσύνη των επενδυτών, γεγονός που με τη σειρά του προκαλεί μείωση των τιμών των μετοχών. Ως εκ τούτου, το κόστος μιας σοβαρής επίθεσης στον κυβερνοχώρο δεν αφορά μόνο την υπονόμευση των εμπιστευτικών δεδομένων, αλλά έχει επίσης άμεσο και διαρκή αντίκτυπο στη συνολική φήμη της εταιρείας. Η ελαχιστοποίηση των επιπτώσεων των κυβερνοεπιθέσεων στην χρηματιστηριακή αξία θα πρέπει να αποτελέσει βασική προτεραιότητα για τις επιχειρήσεις (James, 2018).

Ιδιαίτερο ενδιαφέρον για μελέτη συγκέντρωσαν, επίσης, θέματα που αφορούν το πως αντιμετωπίζουν τον κίνδυνο στον κυβερνοχώρο οι μικρομεσαίες επιχειρήσεις. Πιο συγκεκριμένα, παρατηρείται ότι η ασφάλεια έναντι των απειλών στο Διαδίκτυο δεν αποτελεί βασική προτεραιότητα των μικρομεσαίων εταιριών. Θα ήταν λάθος να θεωρηθεί ότι αυτή η έλλειψη επενδύσεων οφείλεται στην απροσεξία ή στην απαθή στάση τους απέναντι στην ασφάλεια των πληροφοριών. Σε πολλές περιπτώσεις η βασική αιτία είναι η έλλειψη κατανόησης και ευαισθητοποίησης επί του θέματος. Με άλλα λόγια οι μικρομεσαίες επιχειρήσεις δεν κατανοούν ούτε τον κίνδυνο ούτε τις επακόλουθες συνέπειες. Έκτος όμως από αυτό, υπάρχει το πρόβλημα του περιορισμένου χρόνου για εκπαίδευση του προσωπικού και διαθέσιμου προϋπολογισμού προκειμένου να δαπανηθεί για ανάλογο σκοπό. Τέλος, η αισθητή απουσία του νομοθετικού πλαισίου που επιβάλλει συμμόρφωση με συγκεκριμένα πρότυπα, επιβαρύνει την κατάσταση (Goucher, 2011).

Δεν υπάρχει αμφιβολία ότι ο κίνδυνος στον κυβερνοχώρο επηρεάζει τόσο τις μικρές όσο και τις μεγαλύτερες επιχειρήσεις. Παρά το μέγεθος τους, οι μικρές εταιρίες

διαχειρίζονται έναν αρκετά σημαντικό όγκο δεδομένων, γεγονός που τις καθιστά το τέλειο θύμα για τους επίδοξους χάκερ (Kurpjuhn, 2015). Έρευνες έχουν δείξει ότι σε περίπτωση επίθεσης στον κυβερνοχώρο, ένα μεγάλο ποσοστό μικρομεσαίων επιχειρήσεων σταματά την επιχειρηματική του δραστηριότητα σε διάστημα μόλις έξι μηνών. Συνεπώς, οι αρμόδιοι σε κάθε περίπτωση θα πρέπει να λαμβάνουν αντίστοιχα μέτρα με τους οργανισμούς μεγαλύτερου μεγέθους προκειμένου να επιτύχουν την επιθυμητή ασφάλεια. Πολλοί είναι αυτοί που καθιερώνουν το λεγόμενο τείχος ασφαλείας ως μέτρο πρόληψης λόγω περιορισμένων διαθέσιμων οικονομικών πόρων, κάτι που όμως, δεν αποτελεί λύση απέναντι στους αμέτρητους κινδύνους που πιθανόν να αντιμετωπίσει η εταιρία στον κυβερνοχώρο (Caldwell, 2015).

Τα μέτρα τα οποία μπορούν να προσφέρουν ουσιαστικά αποτελέσματα για την προστασία των μικρομεσαίων επιχειρήσεων έναντι των απειλών του διαδικτύου αποτέλεσαν θέμα συζήτησης πολλών αρθρογράφων, καταλήγοντας σε μία λίστα με ορισμένες συμβουλές που οφείλουν να ακολουθούν οι εταιρίες σε τέτοιες περιπτώσεις. Σαφώς, οι οδηγίες αυτές έχουν ως πυρήνα την βελτίωση των εσωτερικών διαδικασιών μιας επιχείρησης καθώς, είναι αυτές που ευθύνονται στο μεγαλύτερο βαθμό για τυχόν αδυναμίες πρόληψης ή αντιμετώπισης ανάλογων περιστάσεων. Το γεγονός αυτό προβληματίζει ιδιαιτέρως τόσο την διοίκηση ενός οργανισμού όσο και τους υπεύθυνους ασφαλείας διαδικτυακών κινδύνων. Εν κατακλείδι, καλό θα είναι οι επιχειρήσεις να ελέγχουν και να αναλύουν τα δεδομένα καταγραφής ενώ παράλληλα να φροντίζουν να βελτιώσουν των εσωτερικό τους έλεγχο, λαμβάνοντας προληπτικά μέτρα όπως οι δικλίδες ασφαλείας των διαδικτυακών τους υπηρεσιών, η θέσπιση ισχυρών κωδικών πρόσβασης και η ενδυνάμωση του τείχους προστασίας τους (Paul, 2017).

2.3.3 Η ασφάλιση έναντι των κίνδυνων του Κυβερνοχώρου (cyber insurance)

Οι παραβιάσεις δεδομένων και τα συμβάντα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο έχουν γίνει σύνηθες φαινόμενο, με χιλιάδες να συμβαίνουν κάθε χρόνο και μερικές να κοστίζουν εκατοντάδες εκατομμύρια δολάρια (Takahashi, 2018). Κατά συνέπεια, η αγορά για την ασφάλιση έναντι αυτών των απωλειών αυξήθηκε ταχέως κατά την τελευταία δεκαετία. Η ασφάλεια στον κυβερνοχώρο είναι ένας ευρύς όρος για ασφαλιστήρια συμβόλαια

που αντιμετωπίζουν ζημίες εξαιτίας επιθέσεων μέσω υπολογιστή ή δυσλειτουργίας των συστημάτων τεχνολογίας πληροφοριών μιας επιχείρησης. Πιο συγκεκριμένα, με την έννοια της επίθεσης εννοείται ένα συμβάν πειρατείας ή μία περίπτωση όπου ένα μη εξουσιοδοτημένο άτομο αποκτά πρόσβαση στο σύστημα υπολογιστών, ή μία επίθεση είτε με τη χρήση ιού ή άλλου κακόβουλου λογισμικού, ή μια επίθεση άρνησης υπηρεσίας κατά του συστήματος (denial of service attack).

Η δραματική αύξηση αυτών των επιθέσεων σε συνδυασμό με την ένταξη των επιχειρήσεων σε μια ψηφιακή οικονομία έχει δημιουργήσει ζήτηση για νέα ασφαλιστικά προϊόντα που αντισταθμίζουν μέρος του κινδύνου στον κυβερνοχώρο. Έτσι, πολλές ασφαλιστικές εταιρείες εισήγαγαν νέες πολιτικές που καλύπτουν τις διάφορες πτυχές του εν λόγω κινδύνου. Κατά τον σχεδιασμό αυτών των νέων συμβολαίων, οι ασφαλιστικές εταιρείες ασχολήθηκαν με θέματα που αφορούν την τιμολόγηση, την δυσμενή επιλογή και τον ηθικό κίνδυνο. Αν και καθένα από αυτά είναι κοινό σε όλες τις μορφές ασφάλισης, η κατάσταση κινδύνου στον κυβερνοχώρο δημιουργεί διαφορετικές ανησυχίες (Gordon, et al., 2003).

Η τιμολόγηση των ασφαλιστικών προϊόντων βασίζεται παραδοσιακά σε αναλογιστικούς πίνακες κατασκευασμένους από ογκώδη ιστορικά αρχεία. Δεδομένου ότι το Διαδίκτυο είναι σχετικά νέο, δεν υπάρχουν εκτεταμένες ιστορίες ηλεκτρονικών εγκλημάτων και συναφών απωλειών. Παρά την κατάσταση αυτή, οι ασφαλιστικές εταιρείες έχουν προβεί σε καθορισμό τιμών για τα συμβόλαιά τους για τον κίνδυνο του κυβερνοχώρου. Ως εκ τούτου, έχουν ποσοτικοποιήσει αυτό που ορισμένοι ισχυρισμοί συνιστούν μη ποσοτικοποιήσιμο κίνδυνο. Ωστόσο, δεδομένης της μεγάλης αβεβαιότητας που συνεπάγεται ο υπολογισμός της αναλογιστικής αξίας των ασφαλιστηρίων συμβολαίων κινδύνου στον κυβερνοχώρο, απομένει να διαπιστωθεί εάν τα εν λόγω συστήματα τιμολόγησης είναι ορθά (Gordon, et al., 2003).

Το δεύτερο στοιχείο που πρέπει να λάβουν υπόψη τους οι ασφαλιστικές εταιρίες κατά τον σχεδιασμό ενός ασφαλιστήριου συμβολαίου είναι η δυσμενής επιλογή. Πιο αναλυτικά, πρόκειται για το πρόβλημα που προκύπτει όταν μια επιχείρηση ή ένα πρόσωπο επιλέγει να ασφαλιστεί έναντι μιας συγκεκριμένης ζημίας για την οποία είναι πιθανό να έχει ιδιωτικές πληροφορίες που δεν είναι διαθέσιμες στην ασφαλιστική εταιρεία κατά τη στιγμή της σύναψης της σύμβασης. Για παράδειγμα, σε σχέση με την ασφάλεια κινδύνου στον κυβερνοχώρο, το πρόβλημα της δυσμενής επιλογής σχετίζεται με την πιθανότητα παραβίασης της ασφάλειας. Οι επιχειρήσεις με μεγαλύτερη πιθανότητα παραβίασης της ασφάλειας των

πληροφοριών θα ήταν πιο επιρρεπείς στην αγορά αυτής της πολιτικής από τις επιχειρήσεις με μικρή πιθανότητα τέτοιας παραβίασης. Για να προστατευθούν από το πρόβλημα της δυσμενής επιλογής όταν προσφέρουν ασφαλιστήρια για κίνδυνο στον κυβερνοχώρο, οι ασφαλιστικές εταιρείες συνήθως απαιτούν έλεγχο ασφάλειας πληροφοριών πριν από την έκδοση ενός ασφαλιστηρίου συμβολαίου. Μια άλλη απάντηση στο πρόβλημα της δυσμενής επιλογής είναι οι ασφαλιστικές εταιρείες να εντοπίζουν χρήστες υψηλού κινδύνου και να διαφοροποιούν τα ασφάλιστρα για τους εν λόγω χρήστες (Gordon, et al., 2003).

Αντίθετα με την δυσμενή επιλογή, το πρόβλημα του ηθικού κινδύνου αφορά την έλλειψη κινήτρων από τον ασφαλισμένο να λάβει μέτρα που μειώνουν την πιθανότητα ζημίας μετά την αγορά της ασφάλισης. Για παράδειγμα, μια επιχείρηση με ασφάλιση έναντι των κινδύνων του κυβερνοχώρου μπορεί να είναι λιγότερο διατεθειμένη να λάβει μέτρα που μειώνουν την εμφάνιση ανάλογων περιστατικών από μια επιχείρηση χωρίς τέτοια ασφάλιση. Ένας τρόπος με τον οποίο τα ασφαλιστήρια συμβόλαια μπορούν να αντιμετωπίσουν το πρόβλημα του ηθικού κινδύνου είναι μέσω της χρήσης ρητρών. Έτσι, ο ασφαλισμένος θα υποστεί κάποια ζημία σε περίπτωση που συμβεί στην πραγματικότητα μια επίθεση. Συνεπώς, το εκπιπτόμενο ποσό παρέχει ένα νομισματικό κίνητρο στον ασφαλισμένο να λάβει μέτρα που μειώνουν την πιθανότητα να συμβεί κάτι τέτοιο (Gordon, et al., 2003).

Με βάση τα παραπάνω γίνεται εύκολα αντιληπτό ότι η συνήθης προσέγγιση για τη διαχείριση του κινδύνου ασφάλειας των πληροφοριών είναι παρόμοια με άλλους επιχειρηματικούς κινδύνους. Σε πρώτο στάδιο γίνεται προσπάθεια από την εταιρία να εξαλείψει τον κίνδυνο, και εφόσον αυτό δεν καταστεί δυνατό προσπαθεί τουλάχιστον να τον μετριάσει. Διαφορετικά τον μεταβιβάζει σε τρίτους. Καθώς η εξάλειψη των κινδύνων ασφαλείας στο σημερινό διαδικτυακό περιβάλλον δεν είναι δυνατή, οι διαχειριστές υλοποιούν τεχνολογίες προστασίας όπως το τείχος προστασίας, η προστασία από ιούς, η κρυπτογράφηση, η αποκατάσταση των πολιτικών ασφάλειας, όπως κωδικούς πρόσβασης, έλεγχο πρόσβασης, αποκλεισμό θυρών κ.λπ. για να μειώσουν την πιθανότητα διάρρηξης ή βλάβης. Εάν ο υπολειπόμενος κίνδυνος είναι διαχειρίσιμος, απορροφάται, διαφορετικά, μεταβιβάζεται είτε με εξωτερική ανάθεση ασφάλειας είτε με αγορά ασφάλισης (Bohme & Kataria, 2006).

Ο αβέβαιος και περίπλοκος χαρακτήρας των επιθέσεων στον τομέα της ασφάλειας στον κυβερνοχώρο είναι μία από τις βασικές προκλήσεις που αντιμετωπίζουν οι οργανισμοί στον σημερινό διασυνδεδεμένο ψηφιακό κόσμο. Ωστόσο, οι οργανισμοί δεν μπορούν

ρεαλιστικά να εξαλείψουν όλους τους κινδύνους για την ασφάλεια στον κυβερνοχώρο και την επίτευξη ασφάλειας σε ποσοστό 100%. Επιπλέον, οι επενδύσεις στον τομέα της ασφάλειας στον κυβερνοχώρο γίνονται τελικά πιο δαπανηρές από τα οφέλη που προκύπτουν από την πρόσθετη ασφάλεια. Ο βασικότερος στόχος των ερευνητών είναι να αναπτύξουν ένα μοντέλο το οποίο θα εξετάζει τις πτυχές κόστους-οφέλους των επενδύσεων στον τομέα της ασφάλειας στον κυβερνοχώρο. Με τον τρόπο αυτό, οι επιχειρήσεις θα μπορούν να επιλέγουν το βέλτιστο σύνολο ασφαλιστήριων συμβολαίων για την προστασία τους στον κυβερνοχώρο ανάμεσα στο πεπερασμένο σύνολο που προσφέρονται από τις ασφαλιστικές εταιρείες. Με άλλα λόγια, θα έχουν την δυνατότητα να επιλέξουν ένα σύνολο ασφαλιστηρίων προκειμένου να ελαχιστοποιήσουν το συνολικό αναμενόμενο κόστος των ασφαλίστρων συν την αναμενόμενη ζημία από μια παραβίαση, ώστε να επιτύχουν μια αποτελεσματική αγορά ασφάλειας στον κυβερνοχώρο (Bodin, et al., 2018).

Είναι γεγονός ότι, παρά την αργή εκκίνηση και τα πολλά προβληματικά ζητήματα, η αγορά ασφάλισης στον κυβερνοχώρο αναπτύσσεται. Αυτή η ανάπτυξη εξαρτάται σε μεγάλο βαθμό από τις ρυθμιστικές πρωτοβουλίες που εφαρμόζονται ευρύτερα στον κόσμο, αλλά αυτή δεν είναι η μόνη αιτία για την ανάπτυξη της αγοράς. Η ασφάλεια στον κυβερνοχώρο από μόνη της παρέχει μια μοναδική ευκαιρία για την κάλυψη των κινδύνων, καθώς και για τη συμβολή στην κοινωνική ευημερία. Ωστόσο, αν και αποτελεί επιλογή για της επιχειρήσεις, έχει πολλά ανοικτά ζητήματα που δεν έχουν επιλυθεί ακόμα από επιστήμονες και επαγγελματίες. Απαιτούνται καινοτόμες προσεγγίσεις για την επίτευξη θετικών αποτελεσμάτων σε σχέση με την ασφάλεια στον κυβερνοχώρο, καθώς και νέα πρότυπα και πρακτικές για την ωρίμανση της αγοράς (Marotta, et al., 2017).

ΚΕΦΑΛΑΙΟ 3

ΚΙΝΔΥΝΟΙ ΚΥΒΕΡΝΟΧΩΡΟΥ

3.1 Ορισμός

Ο όρος "κίνδυνος στον κυβερνοχώρο" αναφέρεται σε μια πληθώρα διαφορετικών πηγών κινδύνου που επηρεάζουν τα περιουσιακά στοιχεία μιας επιχείρησης στον τομέα της πληροφορίας και της τεχνολογίας. Ορισμένα παραδείγματα κινδύνου στον κυβερνοχώρο περιγράφονται από την Εθνική Ένωση Ασφαλιστικών Επιτρόπων και περιλαμβάνουν κλοπή ταυτότητας, γνωστοποίηση ευαίσθητων πληροφοριών και τη διακοπή των επιχειρηματικών δραστηριοτήτων (National Association of Insurance Commissioners (NAIC), 2013). Έχουν γίνει πολλές προσπάθειες ώστε να προσδιοριστεί ο ορισμός του "κινδύνου στον κυβερνοχώρο". Ορισμένες από αυτές χρησιμοποιούν στενές έννοιες. Για παράδειγμα, αναφέρονται στον κίνδυνο στον κυβερνοχώρο ως τον κίνδυνο που ενέχει ένα κακόβουλο ηλεκτρονικό φαινόμενο που προκαλεί διαταραχή των επιχειρήσεων και νομισματική απώλεια (Mukhopadhyay, et al., 2005). Άλλοι υιοθετούν μια ευρύτερη προοπτική ορίζοντάς τον ως κίνδυνο για την ασφάλεια των πληροφοριών (Öğüt, et al., 2011) ή κίνδυνο που οδηγεί σε αποτυχία των συστημάτων πληροφοριών (Böhme & Kataria, 2006). Τέλος, οι κίνδυνοι στον κυβερνοχώρο μπορούν να οριστούν ως «λειτουργικοί κίνδυνοι για στοιχεία της πληροφορίας και της τεχνολογίας που έχουν επιπτώσεις στην εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των πληροφοριακών συστημάτων» (Cebula & Young, 2010).

3.2 Ταξινόμηση κινδύνων κυβερνοχώρου

Η ταξινόμηση των λειτουργικών κινδύνων για την ασφάλεια στον κυβερνοχώρο είναι δομημένη γύρω από μια ιεραρχία κατηγοριών, υποκατηγοριών και στοιχείων. Η ταξινόμηση γίνεται με βάση τέσσερις κύριες κατηγορίες:

- Ενέργειες ατόμων: ενέργειες ή έλλειψη δράσης, που αναλαμβάνονται από άτομα είτε σκόπιμα είτε τυχαία και επηρεάζουν την ασφάλεια στον κυβερνοχώρο.
- Αστοχίες συστημάτων και τεχνολογίας: αστοχία υλικού, λογισμικού και συστημάτων πληροφοριών.
- Αποτυχημένες εσωτερικές διεργασίες: προβλήματα στις εσωτερικές επιχειρηματικές διεργασίες που επηρεάζουν την ικανότητα υλοποίησης, διαχείρισης και διατήρησης της ασφάλειας στον κυβερνοχώρο, όπως σχεδίαση, εκτέλεση και έλεγχος διεργασιών
- εξωτερικά συμβάντα: ζητήματα που συχνά δεν εμπίπτουν στον έλεγχο του οργανισμού, όπως καταστροφές, νομικά ζητήματα, επιχειρηματικά ζητήματα κ.α. (Cebula & Young, 2010)

Καθεμία από τις τέσσερις αυτές κατηγορίες υποδιαιρείται περαιτέρω σε υποκατηγορίες και κάθε υποκατηγορία περιγράφεται από τα στοιχεία της. Είναι σημαντικό να σημειωθεί ότι οι κίνδυνοι σε μια κατηγορία μπορούν να προκαλέσουν κινδύνους σε άλλη κατηγορία. Στην περίπτωση αυτή, η ανάλυση ενός κινδύνου μπορεί να περιλαμβάνει πολλά στοιχεία από διαφορετικές κατηγορίες. Για παράδειγμα, μια αποτυχία του λογισμικού λόγω ακατάλληλων ρυθμίσεων ασφαλείας μπορεί να προκληθεί τόσο εξαιτίας μιας ακούσιας όσο και μιας εκούσιας ενέργειας των ανθρώπων.

3.2.1 Κατηγορία 1η – Ενέργειες ατόμων

Οι ενέργειες των ατόμων περιγράφουν μια κατηγορία λειτουργικού κινδύνου που χαρακτηρίζεται από προβλήματα που προκαλούνται από τις ενέργειες που έχουν αναληφθεί ή δεν έχουν αναληφθεί από άτομα σε μια δεδομένη κατάσταση. Αυτή η κατηγορία καλύπτει ενέργειες τόσο από εσωτερικούς όσο και από εξωτερικούς συνεργάτες και παρουσιάζει τις παρακάτω υποκατηγορίες:

- Ακούσιες

Η υποκατηγορία αυτή αναφέρεται σε μέτρα που λαμβάνονται χωρίς κακόβουλη ή επιβλαβή πρόθεση. Οι ακούσιες ενέργειες συνήθως, αν και όχι αποκλειστικά, σχετίζονται με ένα άτομο στο εσωτερικό του οργανισμού. Μπορεί να πρόκειται για σφάλματα, λάθη ή παραλείψεις.

- Εσκεμμένες

  Η υποκατηγορία αυτή περιγράφει τις ενέργειες που πραγματοποιούνται εκ προθέσεως και με σκοπό να προκαλέσουν βλάβη. Τέτοιες μπορεί να είναι η απάτη, η δολιοφθορά, η κλοπή και ο βανδαλισμός. Οι εσκεμμένες ενέργειες μπορούν να πραγματοποιηθούν είτε από πρόσωπα που κατέχουν εμπιστευτικές πληροφορίες είτε από τρίτους.

- Αδράνειας

  Η υποκατηγορία αυτή περιγράφει την έλλειψη δράσης ή την αδυναμία δράσης σε μια δεδομένη κατάσταση. Κάτι τέτοιο μπορεί να συμβαίνει λόγω έλλειψης κατάλληλων δεξιοτήτων, γνώσεων, καθοδήγησης, ή επιλογής του σωστού ατόμου για την ανάληψη δράσης (Cebula & Young, 2010).

3.2.2 Κατηγορία 2η – Αποτυχίες συστημάτων και τεχνολογίας

Οι αστοχίες συστημάτων και τεχνολογίας περιγράφουν μια κατηγορία λειτουργικού κινδύνου που χαρακτηρίζεται από προβληματική, μη φυσιολογική ή μη αναμενόμενη λειτουργία των πόρων τεχνολογίας και διακρίνεται στις παρακάτω υποκατηγορίες:

- Υλικού

  Η υποκατηγορία αυτή σχετίζεται με βλάβες στον φυσικό εξοπλισμό λόγω χωρητικότητας, απόδοσης, συντήρησης και απαρχαιωμένων εγκαταστάσεων.

- Λογισμικού

  Η υποκατηγορία αυτή περιλαμβάνει κινδύνους που προκύπτουν από πόρους λογισμικού κάθε είδους, συμπεριλαμβανομένων προγραμμάτων, εφαρμογών και λειτουργικών συστημάτων. Παραδείγματα αποτελούν η συμβατότητα, η διαχείριση διαμόρφωσης, ο έλεγχος αλλαγών, οι ρυθμίσεις ασφάλειας, οι πρακτικές κωδικοποίησης και οι δοκιμές.

- Συστημάτων

Η υποκατηγορία αυτή σχετίζεται με τις αποτυχίες των ολοκληρωμένων συστημάτων να λειτουργήσουν όπως αναμενόταν. Αυτές μπορεί να συμβούν εξαιτίας της σχεδίασης, των προδιαγραφών, της ενσωμάτωσης ή της πολυπλοκότητας (Cebula & Young, 2010).

3.2.3 Κατηγορία 3η – Αποτυχημένες εσωτερικές διεργασίες

Οι αποτυχημένες εσωτερικές διεργασίες περιγράφουν μια κατηγορία λειτουργικού κινδύνου που σχετίζεται με προβληματικές αστοχίες των εσωτερικών διεργασιών που πρέπει να εκτελούνται όπως απαιτείται ή αναμένεται. Παρακάτω παρουσιάζεται η ανάλυσή τους σε υποκατηγορίες:

- Σχεδιασμός ή εκτέλεση διεργασίας

  Η υποκατηγορία αυτή αναφέρεται σε αποτυχίες των διεργασιών λόγω του ακατάλληλου σχεδιασμού τους ή λόγω κακής εκτέλεσης μιας σωστά σχεδιασμένης διεργασίας. Παραδείγματα τέτοιων αποτυχιών μπορεί να εντοπίζονται στη ροή της διαδικασίας, στην τεκμηρίωσή της, στους ρόλους και τις ευθύνες που έχουν αποδοθεί, στις ειδοποιήσεις και προειδοποιήσεις, στη ροή των πληροφοριών, στην εξέλιξη των ζητημάτων, στο επίπεδο εξυπηρέτησης συμφωνιών και στην ανάθεση εργασιών.

- Στοιχεία ελέγχου διεργασιών

  Η υποκατηγορία αυτή περιλαμβάνει τις αποτυχίες της διεργασίας λόγω ανεπαρκών ελέγχων στη λειτουργία της διεργασίας. Τα στοιχεία αυτής της υποκατηγορίας είναι η παρακολούθηση κατάστασης, οι μετρήσεις, η περιοδική επανεξέταση, και κατοχή διεργασιών.

- Υποστηρικτικές διεργασίες

  Η υποκατηγορία των διαδικασιών υποστήριξης ασχολείται με λειτουργικούς κινδύνους που έχουν δημιουργηθεί λόγω της αποτυχίας των διαδικασιών οργανωτικής υποστήριξης να παράσχουν τους κατάλληλους πόρους. Οι διαδικασίες υποστήριξης μπορεί να αφορούν το προσωπικό, τη λογιστική, την κατάρτιση και την ανάπτυξη, καθώς και τις προμήθειες (Cebula & Young, 2010).

3.2.4 Κατηγορία 4η – Εξωτερικά συμβάντα

Τα εξωτερικά γεγονότα αποτελούν μια κατηγορία λειτουργικού κινδύνου που σχετίζεται με συμβάντα γενικά εκτός του ελέγχου του οργανισμού. Συχνά, δεν είναι εύκολο να προγραμματιστεί ή να προβλεφθεί ο χρόνος και η εμφάνιση τέτοιων συμβάντων. Οι υποκατηγορίες στις οποίες αναλύονται είναι οι εξής:

- Καταστροφές

  Η υποκατηγορία αυτή περιλαμβάνει γεγονότα, είτε φυσικής είτε ανθρώπινης προέλευσης, για τα οποία ο οργανισμός δεν έχει την δυνατότητα να ασκήσει κανέναν έλεγχο καθώς συνήθως εμφανίζονται δίχως να υπάρχουν προειδοποιητικές ενδείξεις. Για παράδειγμα, καιρικά φαινόμενα, πυρκαγιά, πλημμύρα, σεισμό, κοινωνικές αναταραχές και πανδημία.

- Νομικά ζητήματα

  Η υποκατηγορία αυτή ασχολείται με κινδύνους που ενδέχεται να επηρεάσουν τον οργανισμό λόγω των στοιχείων κανονιστικής συμμόρφωσης, της νομοθεσίας και των δικαστικών υποθέσεων

- Επιχειρηματικά ζητήματα

  Η υποκατηγορία αυτή περιλαμβάνει ζητήματα οικονομικής φύσεως όπως, η ανεπάρκεια των προμηθευτών, οι συνθήκες της αγοράς κ.α.

- Εξάρτηση υπηρεσιών

  Η υποκατηγορία αυτή αναφέρεται σε κινδύνους που προκύπτουν από την εξάρτηση του οργανισμού από εξωτερικά μέρη για τη συνέχιση των λειτουργιών του, παραδείγματος χάρη υπηρεσιών κοινής ωφέλειας, έκτακτης ανάγκης, καύσιμων και μεταφορών (Cebula & Young, 2010).

3.3 Οικονομικές επιπτώσεις κινδύνου κυβερνοχώρου

Η εκτίμηση του κόστους που προκαλείται από τον κίνδυνο στον κυβερνοχώρο είναι δύσκολη, καθώς υπάρχει μεγάλη αβεβαιότητα και καμία αποδεκτή πηγή πληροφοριών. Ορισμένα είδη εγκλήματος στον κυβερνοχώρο ενδέχεται να μην έχουν κανένα κόστος ή να μην μπορούν να ποσοτικοποιηθούν (π.χ. διάδοση του ρατσισμού, παρενόχληση ή εμπορία παράνομων

ναρκωτικών). Ωστόσο, γίνονται προσπάθειες από πολλούς ερευνητές ώστε να εκτιμηθεί το συνολικό κόστος, το κόστος ανά παραβίαση και το κόστος ανά καταγραφή παραβίασης δεδομένων. Το συνολικό κόστος του κινδύνου στον κυβερνοχώρο εκτιμάται γενικά ότι υπερβαίνει τα 100 δισεκατομμύρια δολάρια, γεγονός που τονίζει την οικονομική σημασία του κινδύνου στον κυβερνοχώρο. Ωστόσο, ανάλογα με τον ορισμό που εφαρμόζεται, οι εκτιμήσεις διαφέρουν σημαντικά. Ενώ η Symantec, σε εκτίμησή της το 2013 (113 δισεκατομμυρίων δολαρίων) λαμβάνει υπόψη μόνο τις άμεσες δαπάνες, η McAfee σε ανάλογη εκτίμηση το 2014 (445 δισεκατομμυρίων δολαρίων) ενσωματώνει και έμμεσες δαπάνες, όπως τα έξοδα φήμης για την πληττόμενη εταιρεία. Μέσα από το ευρύ φάσμα που παρείχε η Kshetri σε δική της εκτίμηση το 2010 (από 100 έως 1.000 δισεκατομμύρια δολάρια) είναι εμφανής η αβεβαιότητα που υπάρχει κατά την εκτίμηση του κόστους κινδύνου στον κυβερνοχώρο. Το κόστος ανά παραβίαση δεδομένων που αντιμετωπίζει μια χακαρισμένη εταιρεία παρουσιάζει λιγότερες διακυμάνσεις και εκτιμάται ότι κυμαίνεται μεταξύ 2,1 και 3,8 εκατομμυρίων δολαρίων. Επιπλέον, η απώλεια κάθε εγγραφής (π.χ. του αριθμού πιστωτικής κάρτας) δημιουργεί κόστος από 217 έως 956 δολάρια. Η McAfee παρέχει επίσης εκτιμήσεις για το κόστος κινδύνου στον κυβερνοχώρο σε διαφορετικές χώρες, το οποίο εμφανίζει έντονες διακυμάνσεις μεταξύ τους. Για παράδειγμα, για τις ΗΠΑ το κόστος που αναλογεί είναι 0,64 τοις εκατό του ΑΕΠ ενώ αντιθέτως για την Γερμανία το ποσοστό αυτό φτάνει το 1,6 τοις εκατό (Eling & Schnell, 2016).

Δεδομένων αυτών των ακραίων διακυμάνσεων, φαίνεται ότι οι υπάρχουσες εκτιμήσεις κόστους. κάθε άλλο, παρά αξιόπιστες είναι. Οι αριθμοί αυτοί πρέπει να ερμηνεύονται με προσοχή, καθώς οι περισσότεροι εξ' αυτών έχουν εκτιμηθεί από εταιρείες ασφάλειας και παροχής συμβουλών, οι οποίες ενδέχεται να έχουν μεροληπτική άποψη. Οι αδυναμίες αυτής της μεθοδολογίας έχουν μελετηθεί από διάφορους ερευνητές οι οποίοι προσπάθησαν να δώσουν εναλλακτικές λύσεις. Γενικά, οι συγγραφείς καταλήγουν ότι το ετήσιο κόστος για την παγκόσμια οικονομία είναι εξαιρετικά αβέβαιο. Ορισμένοι από αυτούς υποστηρίζουν, επίσης, ότι το μεγαλύτερο μέρος του κόστους στον κυβερνοχώρο είναι οι έμμεσες ζημίες (π.χ. απώλεια εμπιστοσύνης) και αμυντικά έξοδα (π.χ. λογισμικό προστασίας από ιούς, ασφάλιση), εξαιρουμένων των άμεσων ζημιών (π.χ. κλοπή χρημάτων) (Anderson , et al., 2013).

Τέλος, διάφοροι μελετητές προσπαθούν να αξιολογήσουν τις άμεσες και έμμεσες επιπτώσεις που μπορεί να έχουν τα περιστατικά του κινδύνου στον κυβερνοχώρο στις τιμές των μετοχών των εταιρειών. Για παράδειγμα, σε αντίστοιχη έρευνα υποστηρίζεται ότι η

παραβίαση της ασφάλειας επηρεάζει αρνητικά την τιμή των μετοχών της εταιρείας. Οι εκτιμήσεις μιλούν για ζημία η οποία θα ανέλθει στο 2,1% του όγκου της αγοράς ή 1,65 δις δολάρια ανά παραβίαση ασφαλείας. Αξίζει να σημειωθεί, επίσης, ότι οι τιμές των μετοχών των παρόχων υπηρεσιών ασφάλειας πληροφοριών αυξάνονται κατά μέσο όρο σε αξία κατά 1,3%, ή 1,06 δις δολάρια, μετά την ανακοίνωση της παραβίασης της ασφάλειας άλλης επιχείρησης (Cavusoglu , et al., 2004). Ένα μεγάλο μέρος της πτώσης της τιμής οφείλεται στον κλονισμό της φήμης της εταιρείας (Sinanaj & Muntermann, 2013). Αντιθέτως, ορισμένοι υποστηρίζουν ότι υπάρχουν περιορισμένες αποδείξεις ότι οι παραβιάσεις δεδομένων ή οι επιθέσεις άρνησης υπηρεσίας επηρεάζουν αρνητικά την τιμή των μετοχών μιας εταιρείας. Ωστόσο, αναγνωρίζεται ότι η παραβίαση εμπιστευτικών δεδομένων έχει μεγαλύτερο αρνητικό αντίκτυπο στην τιμή των αποθεμάτων (Campbell, et al., 2003) και ότι υπάρχει αρνητική επίπτωση στην τιμή για τις εταιρείες με επιχειρηματικό μοντέλο που βασίζεται σε μεγάλο βαθμό στο διαδίκτυο (Hovav & D'Arcy, 2003).

3.4 Κατηγορίες των χάκερ

Καθώς η ψηφιακή πτυχή της κοινωνίας γίνεται όλο και πιο σημαντική, η άμυνα της αποκτά όλο και μεγαλύτερη προτεραιότητα. Δισεκατομμύρια δολάρια δαπανώνται κάθε χρόνο για την προστασία των συστημάτων ασφαλείας προκειμένου να αποφευχθούν επιθέσεις κακόβουλων χακερ που δρουν κυρίως με σκοπό το προσωπικό τους όφελος. Οι συγκεκριμένες δαπάνες παρουσιάζουν ανοδική πορεία με την πάροδο του χρόνου. Στην πραγματικότητα, πρόκειται για μια άνιση μάχη, καθώς οι δράστες χρειάζεται να είναι επιτυχημένοι μόνο μία φορά, ενώ οι υπερασπιστές θα πρέπει να είναι επιτυχημένοι κάθε φορά. Επομένως, είναι επιτακτική ανάγκη να γνωρίζουμε όσο το δυνατόν περισσότερα σχετικά με τους επίδοξους δράστες ώστε να είμαστε σε θέση να σχεδιάσουμε κατάλληλα τις αμυντικές μας προσπάθειες. Αυτό σημαίνει ότι πρέπει να είμαστε σε θέση να κατανοήσουμε καλύτερα τους διάφορους τύπους επιτιθέμενων χάκερ και τι είδους απειλές προκαλούν.
Σύμφωνα με πρόσφατο άρθρο του 2018 οι χάκερ διακρίνονται στις παρακάτω κατηγορίες:

- Νέοι χάκερ και μικροεγκληματίες, που είναι γνωστοί με τον όρο "script kiddies", οι οποίοι γενικά δεν κάνουν μεγάλη ζημιά, αλλά μπορούν, για παράδειγμα, να αλλάξουν σοβαρά ή να καταστρέψουν ιστοσελίδες. Στην ουσία, πρόκειται για νέους χάκερ με ελάχιστη πείρα που βασίζονται σε προκατασκευασμένα προγράμματα εκμετάλλευσης

και αρχεία ("scripts") για να διεξάγουν το χακάρισμά τους και δεν τους απασχολεί να μάθουν περαιτέρω για τον τρόπου που αυτά δουλεύουν.

- Εγκληματικές οργανώσεις που επιδιώκουν χρηματικό κέρδος μέσω κλοπής πνευματικής ιδιοκτησίας, οικονομικών πληροφοριών ή λύτρων για κλεμμένα δεδομένα. Κάποιοι, για παράδειγμα, έχουν ειδικευτεί προκειμένου να επιτίθενται σε νοσοκομεία, ή κλέβουν οικονομικά αρχεία όπως πληροφορίες πιστωτικών καρτών.
- Επίμονοι κρατικοί δράστες που προσπαθούν να εμποδίσουν τη λειτουργία οργανισμών και χωρών, και να κλέψουν πνευματική ιδιοκτησία αναζητώντας άμεση εισβολή ή μέσα για να το κάνουν αργότερα.
- Άλλες εταιρείες ή οργανισμοί που ενδέχεται να επιδιώκουν να επωφεληθούν από την πρόκληση ζημίας σε ανταγωνιστή ή την κλοπή της πνευματικής ιδιοκτησίας του μέσω κατασκοπείας.
- Τρομοκρατικές οργανώσεις που μπορεί να έχουν ως στόχο να προκαλέσουν τη μέγιστη ζημία στις κοινωνίες και να αποκτήσουν χρήματα για τη διατήρηση των οικονομικών τους δραστηριοτήτων.
- Κακόβουλα πρόσωπα όπως για παράδειγμα δυσαρεστημένους υπαλλήλους ή άτομα των οποίων οι αξίες δεν είναι ευθυγραμμισμένες με εκείνες του οργανισμού ή ανθρώπων που απλά επιδιώκουν νομισματικά οφέλη.
- Ανάδοχοι, όπως οι εταιρείες συντήρησης, που έχουν ή βρίσκουν πρόσβαση στο εσωτερικό δίκτυο πληροφοριών για να διαταράξουν τον οργανισμό, είτε ως καθαρή κακομεταχείριση είτε για να πωλήσουν τις κλεμμένες πληροφορίες (Pate-Cornell, et al., 2018).

Επιπρόσθετα, αβεβαιότητα προκαλεί στον επιχειρηματικό κόσμο η αδυναμία των συστημάτων τους και τα σημεία εισόδου μέσω των οποίων οι δράστες μπορούν να διεισδύσουν σε αυτά, όπως για παράδειγμα:

- Ακούσια ελαττώματα ή "σφάλματα" στο λογισμικό που ενδέχεται να παρουσιάστηκαν κατά τον αρχικό προγραμματισμό.
- Εκούσια ελαττώματα που ενδέχεται να εισαχθούν στο υλικό ή το λογισμικό υπολογιστών κατά μήκος της αλυσίδας εφοδιασμού από πιθανούς επιτιθέμενους με σκοπό να τα χρησιμοποιήσουν αργότερα.
- Περιφερειακά ελαττώματα ή "σφάλματα" σε συστήματα εκτός του ελέγχου του υπεύθυνου λήψης αποφάσεων τα οποία μπορούν να εισαχθούν μέσω εξοπλισμού συνδεδεμένου στο κύριο σύστημα (Pate-Cornell, et al., 2018).

3.5 Μέτρα προστασίας απέναντι στους κινδύνους του κυβερνοχώρου

Είναι επιτακτική ανάγκη για όσους είναι επιφορτισμένοι με τη διοίκηση τόσο μιας επιχείρησης όσο και ενός δημόσιου οργανισμού να ευαισθητοποιηθούν για θέματα σχετικά με την ασφάλεια στον κυβερνοχώρο σε όλα τα επίπεδα. Η προστασία του κυβερνοχώρου και η διαχείριση των κινδύνων αποτελούν κοινή ευθύνη κάθε εργαζομένου και ολόκληρης της επιχείρησης. Οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται ταχύτατα και να αυξάνουν την πολυπλοκότητά τους κάθε μέρα, απαιτώντας από την ηγεσία ενός οργανισμού, από τρίτους παρόχους υπηρεσιών, και τους υπαλλήλους, όχι μόνο να είναι προετοιμασμένοι για το πώς να ανταποκριθούν σε μια επικείμενη επίθεση ή παραβίαση, αλλά επίσης να παραμείνουν ένα βήμα μπροστά από νέες ή άγνωστες αδυναμίες. Μια συνήθης επιχειρηματική προσέγγιση στη διαχείριση του κινδύνου στον κυβερνοχώρο δεν είναι πλέον ικανή να επιτύχει αυτούς τους στόχους.

Συνεπώς, η πραγματικότητα είναι ότι ο κίνδυνος στον κυβερνοχώρο δεν είναι κάτι που μπορεί να αποφευχθεί αλλά αντιθέτως, πρέπει να αντιμετωπιστεί. Οι οργανισμοί θα πρέπει να διασφαλίζουν ότι κατανοούν όλα τα δεδομένα που συλλέγονται, τον τρόπο συλλογής τους, τον τόπο αποθήκευσης των δεδομένων αυτών και στη συνέχεια να εστιάζουν στα σημαντικότερα δεδομένα τους για την ανάπτυξη των κατάλληλων ελέγχων ασφαλείας και άλλων μέτρων μετριασμού του κινδύνου για την προστασία των πληροφοριακών στοιχείων, της επωνυμίας και της φήμης του οργανισμού, των αλυσίδων εφοδιασμού κ.λπ. Τα ουσιαστικότερα στοιχεία που πρέπει να επικεντρωθούν ώστε να επιτύχουν την διαχείριση του κινδύνου είναι τα εξής:

- Διακυβέρνηση και πολιτισμός: Η διακυβέρνηση και ο πολιτισμός από κοινού αποτελούν τη βάση για όλες τις άλλες συνιστώσες της διαχείρισης του κινδύνου. Η διακυβέρνηση θέτει το ύφος της οντότητας, ενισχύοντας τη σημασία της επαγρύπνησης στον κυβερνοχώρο και καθιερώνοντας αρμοδιότητες εποπτείας για την οντότητα.
- Στρατηγική και καθορισμός στόχων: Η διαχείριση του κινδύνου στον κυβερνοχώρο ενσωματώνεται στο στρατηγικό σχέδιο της οντότητας μέσω της διαδικασίας καθορισμού της στρατηγικής και των επιχειρηματικών στόχων. Με την κατανόηση του επιχειρηματικού πλαισίου, ο οργανισμός μπορεί να αποκτήσει γνώση των εσωτερικών και εξωτερικών παραγόντων και των επιπτώσεών τους στον κίνδυνο. Έτσι, μπορεί να προχωρήσει στη χάραξη της ανάλογης

στρατηγικής. Οι επιχειρηματικοί στόχοι επιτρέπουν την υλοποίηση της ανάλογης στρατηγικής και τη διαμόρφωση των καθημερινών δραστηριοτήτων και προτεραιοτήτων της οντότητας.

- Απόδοση: Ένας οργανισμός προσδιορίζει και αξιολογεί τους κινδύνους που μπορεί να επηρεάσουν την ικανότητά του να επιτύχει τους στόχους στρατηγικής και επιχειρηματικής του δραστηριότητας. Στο πλαίσιο αυτής της επιδίωξης, ο οργανισμός εντοπίζει και αξιολογεί τους κινδύνους στον κυβερνοχώρο που ενδέχεται να επηρεάσουν την επίτευξη αυτής της στρατηγικής και των επιχειρηματικών στόχων. Δίνει προτεραιότητα στους κινδύνους ανάλογα με τη σοβαρότητά τους και λαμβάνοντας υπόψη το πόσο εκτεθειμένη είναι η οικονομική οντότητα στον κυβερνοχώρο. Ως αποτέλεσμα του ελέγχου της απόδοσης είναι να αναπτύσσεται μια εικόνα του ποσοστού του κινδύνου που η εταιρεία ανέλαβε προκειμένου να επιτευχθούν οι στόχοι της.
- Αναθεώρηση: Εξετάζοντας τις δυνατότητες και τις πρακτικές διαχείρισης του κινδύνου του κυβερνοχώρου και τις επιδόσεις της οικονομικής οντότητας σε σχέση με τους στόχους της, ο οργανισμός μπορεί να εξετάσει πόσο καλά ανταποκρίνεται σε αυτές.
- Πληροφόρηση, επικοινωνία και υποβολή εκθέσεων: Η επικοινωνία είναι η συνεχής, επαναληπτική διαδικασία απόκτησης πληροφοριών και κοινοποίησή τους σε ολόκληρη την οντότητα. Η διοίκηση χρησιμοποιεί σχετικές πληροφορίες τόσο από εσωτερικές όσο και από εξωτερικές πηγές για την υποστήριξη της διαχείρισης του κινδύνου στον κυβερνοχώρο. Ο οργανισμός αξιοποιεί τα συστήματα πληροφοριών για την καταγραφή, επεξεργασία και διαχείριση δεδομένων και πληροφοριών. Χρησιμοποιώντας πληροφορίες που ισχύουν για όλα τα στοιχεία, ο οργανισμός προσδιορίζει τον κίνδυνο, την κουλτούρα και τις επιδόσεις του (Galligan, et al., 2019).

ΚΕΦΑΛΑΙΟ 4

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

4.1 Εισαγωγή

Η συνεχής εξέλιξη του ψηφιακού περιβάλλοντος απέφερε αδιαμφισβήτητα πολλά οφέλη, αυξάνοντας την ποιότητα των δραστηριοτήτων μας και επιταχύνοντας την οικονομική ανάπτυξη. Ο κόσμος, όπως τον βλέπουμε σήμερα, βασίζεται στην τεχνολογική πρόοδο, η οποία άλλαξε κατά τις τελευταίες δεκαετίες, οδηγώντας σε τεράστιο αριθμό αποθηκευμένων και κοινών δεδομένων, στο πλαίσιο της διαδικασίας δημιουργίας αξίας.

Νέες μέθοδοι που διευκόλυναν την αυτοματοποίηση και ενίσχυσαν την ποιότητα των δραστηριοτήτων, άρχισαν να υιοθετούνται ως ένα νέο βήμα προς την ψηφιακή οικονομία και την εξέλιξη των τεχνολογιών που αποθηκεύουν και χειρίζονται τα δεδομένα ως βάση για τις διαδικασίες λήψης αποφάσεων. Ωστόσο, τα νέα για τις παραβιάσεις δεδομένων (που προέρχονται από εταιρείες όπως η Yahoo, η Uber κ.α) επισημαίνουν σαφώς ότι μερικές φορές παραμελούμε να προστατεύσουμε ένα από τα σημαντικότερα ανταγωνιστικά πλεονεκτήματα: την προστασία των προσωπικών δεδομένων. Επιπλέον, αυτά τα περιστατικά αποδεικνύουν ότι όλες οι εταιρείες, ανεξαρτήτως μεγέθους, πρέπει να γνωρίζουν ότι μπορούν να βιώσουν, οποιαδήποτε στιγμή, μια κυβερνοεπίθεση.

Σε επίπεδο Ευρωπαϊκής Ένωσης υπήρχε η οδηγία 95/46/ΕΚ που εγκρίθηκε το 1995 σχετικά με την ασφάλεια των προσωπικών δεδομένων. Παρ' όλα αυτά, κατά τη διάρκεια των ετών, τα πράγματα έχουν αλλάξει δραματικά μαζί με την ανάγκη για ένα καλύτερο πλαίσιο προστασίας της ιδιωτικής ζωής. Προκειμένου να αντιμετωπιστεί η υφιστάμενη εξέλιξη των τεχνολογιών και να παρασχεθεί επαρκές επίπεδο προστασίας, τέθηκε σε ισχύ ένας νέος κανονισμός, ο οποίος ξεκίνησε τον Μάιο του 2018. Αυτός ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR) επεκτείνει τους προηγούμενους κανόνες, ενισχύοντας την ανάγκη για επίγνωση των παραβιάσεων των δεδομένων προσωπικού χαρακτήρα, τη

συμμόρφωση και τη λογοδοσία. Τα τελευταία δύο χρόνια, αυτός ο κανονισμός εξακολουθεί να δημιουργεί ανησυχία στην πλειονότητα των εταιρειών παγκοσμίως, καθώς επηρεάζει βασικές διαδικασίες και οι συνέπειες μη συμμόρφωσης δεν μπορούν να αγνοηθούν.

4.2 Ορισμοί

Στο άρθρο 4 του Κανονισμού καθορίζονται οι έννοιες «δεδομένα προσωπικού χαρακτήρα», «επεξεργασία», «υπεύθυνος επεξεργασίας» και «εκτελών την επεξεργασία» οι οποίες θα χρησιμοποιηθούν στο παρόν Κεφάλαιο και αναλύονται ως εξής:

i. Τα «**δεδομένα προσωπικού χαρακτήρα**» αποτελούν «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»,

ii. Η «**επεξεργασία**» είναι «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»,

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

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

4.3 Τα βασικά χαρακτηριστικά και οι θεμελιώδεις αρχές του Κανονισμού

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων διαθέτει πέντε κύρια χαρακτηριστικά:

i. Εφαρμόζεται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα δίχως εξαιρέσεις σχετικές με το μέγεθος ή τον κλάδο δραστηριότητας
ii. Έχει καθολική εφαρμογή και υποχρεωτικό χαρακτήρα από τις 25 Μάϊου 2018
iii. Σε ορισμένα σημεία παραπέμπει σε Οδηγία καθώς δίνει κατευθυντήριες γραμμές αφήνοντας, παράλληλα, το κάθε κράτος – μέλος να προσαρμόσει τους κανόνες αυτούς στη δική του νομοθεσία
iv. Τα διοικητικά πρόστιμα που προβλέπονται ανάλογα με την παραβίαση του Κανονισμού χαρακτηρίζονται ως ιδιαίτερα υψηλά και μπορούν να αγγίξουν έως τα 20 εκ. ή το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών
v. Αποτελεί «προϊόν» έντονων και πολυετών διαπραγματεύσεων με τεράστια σπουδαιότητα και οικονομικές επεκτάσεις (Ομάδας Εργασίας του ΣΕΒ, 2018).

Επιπλέον, σύμφωνα με το άρθρο 5 του Κανονισμού, ορίζονται οι βασικές αρχές σύμφωνα με τις οποίες πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, οι οποίες είναι οι ακόλουθες:

i. **Η αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας** η οποία πρέπει να χαρακτηρίζει κάθε επεξεργασία προσωπικών δεδομένων καθώς απαιτείται να είναι σύννομη, θεμιτή και να διέπεται από πλήρη διαφάνεια.
ii. **Η αρχή του σκοπού** σύμφωνα με την οποία τα δεδομένα που συλλέγονται αφορούν νόμιμους και καθορισμένους σκοπούς ενώ δεν θα πρέπει να υποβάλλονται σε περεταίρω επεξεργασία εκτός αν πρόκειται για περιπτώσεις που απαιτούνται από το δημόσιο συμφέρον ή περιπτώσεις έρευνας, για παράδειγμα, επιστημονικής ή ιστορικής ή στατιστικής.
iii. **Η αρχή ελαχιστοποίησης των δεδομένων** που εκπληρώνεται όταν τα δεδομένα που υποβάλλονται σε επεξεργασία είναι συναφή και κατάλληλα με τους σκοπούς

για τους οποίους πραγματοποιείται η συλλογή τους και περιορίζονται στα απολύτως αναγκαία.

iv. **Η αρχή της ακρίβειας**, δηλαδή η συλλογή επικαιροποιημένων δεδομένων τα οποία πρέπει να ενημερώνονται διαρκώς και να διαγράφονται ή να διορθώνονται σε περιπτώσεις όπου υπάρχουν ανακρίβειες.

v. **Η αρχή του περιορισμού της περιόδου αποθήκευσης**, η οποία εφαρμόζεται κατά την διάρκεια διατήρησης των δεδομένων και δεν πρέπει να υπερβαίνει το διάστημα που απαιτεί η επεξεργασία των δεδομένων αυτών. Εξαίρεση στα παραπάνω αποτελούν, για ακόμη μία φορά, οι περιπτώσεις όπου απαιτείται από το δημόσιο συμφέρον ή περιπτώσεις έρευνας, για παράδειγμα, επιστημονικής ή ιστορικής ή στατιστικής.

vi. **Η αρχή της ακεραιότητας και εμπιστευτικότητας** που επιβάλλει να πραγματοποιείται η επεξεργασία κατά τρόπο ασφαλή και να παρέχεται η ανάλογη προστασία από τυχαία απώλεια, μη εξουσιοδοτημένη χρήση ή παράνομη επεξεργασία, φθορά ή καταστροφή, με τη λήψη όλων των απαραίτητων μέτρων και

vii. Τέλος, **η αρχή της λογοδοσίας,** η οποία ορίζει τον υπεύθυνο επεξεργασίας ως το άτομο το οποίο φέρει την ευθύνη να αποδείξει τόσο την συμμόρφωση στις απαιτήσεις που θέτει ο Κανονισμός όσο και την ετοιμότητά τους προς συμμόρφωση σε αυτές.

4.4 Ποινές – Κυρώσεις

Είναι γεγονός ότι οι ποινές και οι κυρώσεις που προβλέπονται από τον Κανονισμό χαρακτηρίζονται ιδιαιτέρως αυστηρές και αποτελούν σίγουρα έναν από τους λόγους που η εφαρμογή του έλαβε τόσο μεγάλη δημοσιότητα. Οι νέες υποχρεώσεις των υπευθύνων ήταν κάτι που αναστάτωσε την αγορά και οδήγησε σε αυξημένες δράσεις ενημέρωσης των αρμοδίων είτε στον ιδιωτικό είτε στον δημόσιο τομέα. Ωστόσο, σκοπός του Γενικού κανονισμού είναι κατά κύριο λόγο η πρόληψη και η προστασία των προσωπικών δεδομένων παρά η επιβολή δυσβάσταχτων κυρώσεων. Παρ' όλα αυτά, στο κείμενο του Κανονισμού ορίζονται επακριβώς τα διοικητικά πρόστιμα σε αντίθεση με την Οδηγία 95/46/ΕΚ, η οποία άφηνε στην διακριτική ευχέρεια του νομοθέτη των κρατών μελών να υιοθετήσει τα

κατάλληλα μέτρα συμμόρφωσης ως προς την προστασία των προσωπικών δεδομένων. Σύμφωνα με το άρθρο 84 του Κανονισμού, ο νομοθέτης πλέον μπορεί να ορίζει μόνο τις ποινικές κυρώσεις.

Αναλυτικότερα, τα διοικητικά πρόστιμα αναφέρονται στο άρθρο 83 του Κανονισμού και έχουν διαβαθμίσεις ανάλογα με την σοβαρότητα της παράβασης. Όταν πρόκειται για παράβαση η οποία οφείλεται στον υπεύθυνο επεξεργασίας το ποσό του προστίμου μπορεί να ανέλθει έως τα 10.000.000 ευρώ ενώ αν πρόκειται παράβαση της επιχείρησης, το ποσό αυτό αγγίζει έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο. Τα παραπάνω πρόστιμα αυξάνονται έως το ποσό των 20.000.000€ ή, για επιχειρήσεις, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο, για παραβάσεις που αφορούν τις βασικές αρχές για την επεξεργασία, τα δικαιώματα των υποκειμένων των δεδομένων, τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη τρίτη χώρα ή σε διεθνή οργανισμό, οποιαδήποτε υποχρέωση απορρέει από το δίκαιο του κράτους μέλους για τις ειδικές περιπτώσεις επεξεργασίας, και τη μη συμμόρφωση της κυκλοφορίας των δεδομένων σε εντολές που τους επιβάλει η αρμόδια εποπτική αρχή.

4.5 Παραδείγματα ποινών – προστίμων

Παρά την καθολική εφαρμογή του Κανονισμού από τις 25 Μαΐου του 2018, δεν ήταν λίγες οι περιπτώσεις υπέρογκων προστίμων που επιβλήθηκαν από τις αρμόδιες αρχές προστασίας προσωπικών δεδομένων σε διάφορα κράτη μέλη της Ευρωπαϊκής Ένωσης. Παρακάτω παραθέτουμε τα μεγαλύτερα ποσά ποινών που έχουν βεβαιωθεί το 2019 με χρονολογική σειρά:

1. **Πρόστιμο ύψους 50.000.000 ευρώ – Ιανουάριος 2019**

   Το πρόστιμο αυτό έγινε ευρέως γνωστό καθώς επιβλήθηκε στην Google από τις Γαλλικές ρυθμιστικές υπηρεσίες προστασίας δεδομένων (CNIL) για παραβάσεις που σχετίζονται κυρίως με την στοχευμένη προβολή διαφημίσεων. Πιο συγκεκριμένα, κατηγορήθηκε για απουσία διαφάνειας και ενημέρωσης σύμφωνα με τα άρθρα 12 & 13, καθώς και απουσία νόμιμης βάσης επεξεργασίας σύμφωνα με το άρθρο 6 του Γενικού Κανονισμού (Anon., 2019). Η CNIL ανέφερε ότι ο η Google δεν προσπάθησε

αρκετά ώστε να λάβει τη συγκατάθεση των χρηστών πριν την επεξεργασία των δεδομένων. Αντιθέτως, δήλωσε ότι οι άνθρωποι σε μεγάλο βαθμό δεν γνωρίζουν τα δεδομένα που συμφωνούν να μοιραστούν, ή τον τρόπο με τον οποίο η Google σκοπεύει να χρησιμοποιήσει αυτές τις πληροφορίες. Σε δήλωση τους οι γαλλικές αρχές τόνισαν ότι οι υπηρεσίες του κολοσσού έρευνας «μπορούν να αποκαλύψουν σημαντικά μέρη της ιδιωτικής ζωής των χρηστών, καθώς βασίζονται σε τεράστιο αριθμό δεδομένων, μεγάλη ποικιλία υπηρεσιών και σχεδόν απεριόριστους πιθανούς συνδυασμούς». Ωστόσο, το πρόστιμο των 50.000.000 ευρώ είναι πολύ χαμηλότερο από τη μέγιστη ποινή σύμφωνα με τον Ευρωπαϊκό νόμο περί ιδιωτικότητας, η οποία ανέρχεται στο 4 τοις εκατό των παγκόσμιων εσόδων. Για την Google, αυτό θα ήταν πάνω από 4 δισεκατομμύρια δολάρια (Satariano, 2019).

2. **Πρόστιμο ύψους 170.000 ευρώ– Μάρτιος 2019**

Το συμβάν που αναλύεται παρακάτω δεν αφορά διοικητικό πρόστιμο σε εταιρία του ιδιωτικού τομέα, αλλά σε δημόσιο φορέα. Πιο συγκεκριμένα, η Νορβηγική Αρχή Προστασίας Δεδομένων (Datatilsynet) επέβαλε ποινή ύψους 1,6 εκατ. NOK, η οποία ισοδυναμεί με 170.000 ευρώ, στον Δήμο Bergen για παραβιάσεις τόσο του άρθρου 5 όσο και του άρθρου 32 του GDPR. (Anon., 2019). Λόγω ανεπαρκών μέτρων ασφαλείας, ηλεκτρονικά αρχεία στο σύστημα υπολογιστών του δήμου, τα οποία περιείχαν προσωπικά στοιχεία περισσότερων από 35.000 μαθητών των δημοτικών σχολείων του δήμου ήταν προσβάσιμα οποιονδήποτε χρήστη του συστήματος, ανεξάρτητα από τον τύπο εξουσιοδότησης. Το γεγονός ότι η πλειονότητα των θιγόμενων ατόμων ήταν παιδιά και ότι ο δήμος είχε προειδοποιηθεί αρκετές φορές (τόσο από την αρχή όσο και από εσωτερικό πληροφοριοδότη) αποτέλεσε επιβαρυντικό παράγοντα. Η Datatilsynet έλαβε την απόφασή της τον Μάρτιο του 2019, και στις 4 Απριλίου 2019, ο δήμος δήλωσε σε συνέντευξη τύπου ότι δεν επιθυμεί να ασκήσει έφεση κατά της απόφασης (Krog, 2019).

3. **Πρόστιμο ύψους 200.000 ευρώ– Ιούνιος 2019**

Το φθινόπωρο του 2018, η Δανική Υπηρεσία Προστασίας Δεδομένων πραγματοποίησε εποπτική επίσκεψη στη δανική εταιρεία επίπλων IDDesign. Ένα από τα ερωτήματα στα οποία επικεντρώθηκε η επίσκεψη ήταν αν η εταιρεία είχε ορίσει προθεσμίες για τη διαγραφή των στοιχείων των πελατών και αν τηρήθηκαν οι

προθεσμίες αυτές (Anon., 2019). Πριν από την επιθεώρηση, η IDdesign είχε παράσχει μια επισκόπηση των συστημάτων που χρησιμοποιεί η εταιρεία για την επεξεργασία των προσωπικών δεδομένων. Αυτή η επισκόπηση αποκάλυψε ότι ορισμένα από τα καταστήματα επίπλων χρησιμοποιούσαν ένα παλαιότερο σύστημα, σε αντίθεση με τα υπόλοιπα στα οποία αυτό είχε αντικατασταθεί από νεότερο σύστημα. Στο παλιό σύστημα συγκεντρώθηκαν πληροφορίες για τα ονόματα, τις διευθύνσεις, τους αριθμούς τηλεφώνου, τις διευθύνσεις e-mail και το ιστορικό αγορών περίπου 385.000 πελατών. Κατά τη διάρκεια της επιθεώρησης, η IDdesign ανέφερε επίσης ότι τα προσωπικά δεδομένα στο παλαιό σύστημα δεν είχαν διαγραφεί ποτέ. Έτσι, η δανική εποπτική αρχή πρότεινε πρόστιμο ίσο με 1,5 εκατ. DKK ((£180.000) διότι το GDPR ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να αποθηκεύονται για μεγαλύτερο χρονικό διάστημα από αυτό που απαιτεί η επεξεργασία τους. Η IDdesign δεν ανέφερε πότε ότι τα δεδομένα προσωπικού χαρακτήρα στο παλαιό σύστημα δεν είναι πλέον απαραίτητα για σκοπούς επεξεργασίας και, ως εκ τούτου, δεν καθόρισε τις προθεσμίες που ισχύουν για τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο σύστημα αυτό. Συνεπώς, δεν είχε συμμορφωθεί με τις απαιτήσεις του Γενικού Κανονισμού (Jay, 2019).

4. Πρόστιμο ύψους 130.000 ευρώ– Ιούνιος 2019

Η Εθνική Εποπτική Αρχή της Ρουμανίας διενήργησε έρευνα στην UNICREDIT BANK S.A. και διαπίστωσε παράβαση των διατάξεων του άρθρου 25 παράγραφος 1 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου, για την προστασία των φυσικών προσώπων έναντι στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η τράπεζα τιμωρήθηκε με πρόστιμο ύψους 613.912 Lei το οποίο ισοδυναμεί με 130.000 ευρώ. Η κύρωση εφαρμόστηκε στην UNICREDIT BANK SA καθώς δεν εφάρμοζε τα κατάλληλα τεχνικά και οργανωτικά μέτρα τόσο στο πλαίσιο του προσδιορισμού των μέσων επεξεργασίας όσο και των ίδιων των πράξεων επεξεργασίας, προκειμένου να ικανοποιηθούν οι απαιτήσεις του GDPR και να προστατευθούν τα δικαιώματα των υποκειμένων των δεδομένων. Αυτό οδήγησε στην αποκάλυψη δεδομένων σχετικά με τον προσωπικό αριθμό αναγνώρισης και τη διεύθυνση των προσώπων που πραγματοποιούσαν πληρωμές στην UNICREDIT BANK SA, μέσω ηλεκτρονικών συναλλαγών, στον δικαιούχο της συναλλαγής για 337.042 υποκείμενα δεδομένων, κατά την περίοδο από τις 25 Μαΐου 2018 έως τις 10

Δεκεμβρίου 2018. Η κύρωση επιβλήθηκε μετά από κοινοποίηση προς την Εθνική Εποπτική Αρχή στις 22 Νοεμβρίου 2018 (Anon., 2019).

5. **Πρόστιμο ύψους 220.000.000 ευρώ – Ιούλιος 2019**

Το συγκεκριμένο ποσό αποτελεί το υψηλότερο ποσό που δημοσιεύτηκε στην ιστοσελίδα του ΕΣΠΔ, το οποίο όμως, αναφέρεται σε πρόθεση της εποπτικής αρχής για επιβολή του ανωτέρω προστίμου. Για το δεδομένο περιστατικό ευθύνεται η αεροπορική εταιρεία British Airways, η οποία βρέθηκε αντιμέτωπη με την Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου (ICO) για παραβάσεις σχετικές με την ιστοσελίδα της αεροπορικής (Anon., 2019). Μετά από έρευνα της τελευταίας, μέσω της εν λόγω ιστοσελίδας γινόταν εκτροπή των επισκεπτών σε άλλο κακόβουλο ιστότοπο. Με τον τρόπο αυτό τέθηκαν σε κίνδυνο ευαίσθητα στοιχεία όπως ονόματα, διευθύνσεις, αριθμοί καρτών πληρωμών, πληροφορίες κρατήσεων καθώς και στοιχεία σύνδεσης περίπου 5.000 χρηστών. Εκτός αυτού, εντοπίστηκαν γενικότερα θέματα ασφαλείας της σελίδας της αεροπορικής εταιρείας, τα οποία στη συνέχεια επιλύθηκαν σε συνεργασία με την ICO. Εν αναμονή βρίσκεται η επιβολή του οριστικού προστίμου για την υπόθεση αυτή (Lunden, 2019).

6. **Πρόστιμο ύψους 150.000 ευρώ – Ιούλιος 2020**

Απαντώντας σε καταγγελία, η Ελληνική DPA διεξήγαγε αυτεπάγγελτη έρευνα σχετικά με τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα των υπαλλήλων που εργάζονται στην PwC. Σύμφωνα με την καταγγελία, οι εργαζόμενοι έπρεπε να δώσουν τη συγκατάθεσή τους για επεξεργασία των προσωπικών τους δεδομένων. Μετά την έρευνα, το Ελληνικό DPA κατέληξε στο συμπέρασμα ότι η PWC, ως υπεύθυνος επεξεργασίας, είχε επεξεργαστεί παράνομα τα προσωπικά δεδομένα των υπαλλήλων της "κατά παράβαση των διατάξεων του άρθρου 5 του GDPR, δεδομένου ότι χρησιμοποιούσε ακατάλληλη νομική βάση" (Anon., 2019). Επιπλέον, εξήγαγε το συμπέρασμα ότι η PwC επεξεργάστηκε άδικα και χωρίς διαφάνεια τα δεδομένα προσωπικού χαρακτήρα των υπαλλήλων της, παρέχοντάς τους την εσφαλμένη εντύπωση ότι τα δεδομένα τους υφίστανται επεξεργασία βάσει της νομικής βάσης της συγκατάθεσης, σύμφωνα με το GDPR, ενώ στην πραγματικότητα τα δεδομένα τους υφίστανται επεξεργασία βάσει διαφορετικής νομικής βάσης, για την οποία οι εργαζόμενοι δεν είχαν ενημερωθεί. Κατά συνέπεια, η ελληνική εποπτική

αρχή επέβαλε πρόστιμο, σύμφωνα με το άρθρο 83 του Γενικού Κανονισμού, ύψους 150.000 ευρώ. Επιπλέον, της επιβλήθηκαν διορθωτικά μέτρα τα οποία έπρεπε να πραγματοποιήσει εντός διαστήματος τριών μηνών. Το ειρωνικό της υπόθεσης είναι ότι η PwC είναι η απ' τις πρώτες εταιρείες παροχής συμβουλών στους πελάτες της προκειμένου να συμμορφωθούν με τις απαιτήσεις του GDPR, ενώ η ίδια δεν ήταν σε θέση να τις εφαρμόσει (Narendra, 2019).

7. Πρόστιμο ύψους 645.000 ευρώ – Σεπτέμβριος 2019

Μία ακόμη περίπτωση είναι αυτή της Morele.net για οποία η πολωνική αρχή προστασίας δεδομένων ("UODO") εξέδωσε απόφαση επιβολής προστίμου 645.000 ευρώ. Το σημαντικότερο στην υπόθεση αυτή είναι ότι η Morele.net έπεσε θύμα ενός χάκερ, ο οποίος απέκτησε πρόσβαση στη βάση δεδομένων του καταστήματος με περίπου 2,2 εκατομμύρια αρχεία, συμπεριλαμβανομένων σχεδόν 35 χιλιάδων τα οποία περιείχαν ευαίσθητες πληροφορίες που συλλέχθηκαν σε αιτήσεις για δάνεια (Anon., 2019). Τα κλεμμένα δεδομένα, όπως οι τηλεφωνικοί αριθμοί και το ιστορικό αγορών, χρησιμοποιήθηκαν αργότερα για την πλαστογράφηση των πελατών, αποστέλλοντάς τους γραπτά μηνύματα εκ μέρους του καταστήματος, ζητώντας πρόσθετη πληρωμή για την οριστικοποίηση της συναλλαγής τους και ανακατευθύνοντάς τα σε μια ψεύτικη ιστοσελίδα συγκέντρωσης πληρωμών για να κλέψουν περισσότερες πληροφορίες, π.χ. δεδομένα τραπεζικού ελέγχου ταυτότητας. Στην απόφαση της UODO αναφέρεται ένας μακροσκελής κατάλογος των διατάξεων του GDPR που παραβιάστηκαν. Παρ' όλα αυτά, όμως, κατά τον καθορισμό του ποσού του προστίμου, ο πρόεδρος της UODO έλαβε υπόψη ελαφρυντικές περιστάσεις, όπως: ενέργειες της εταιρείας για τον τερματισμό της παράβασης, καλή συνεργασία με τον υπεύθυνο επεξεργασίας και το γεγονός ότι η εταιρεία δεν έχει παραβιάσει προηγουμένως τη νομοθεσία περί προστασίας των προσωπικών δεδομένων (Muciak, 2019).

8. Πρόστιμο ύψους 200.000 ευρώ επί 2 – Οκτώβριος 2019

Η Ελληνική Αρχή Προστασίας Δεδομένων εξέδωσε δύο αποφάσεις στις 7 Οκτωβρίου 2019, βάσει των οποίων επέβαλε δύο διοικητικά πρόστιμα ύψους 200.000 ευρώ έκαστα στον Ελληνικό Πάροχο Τηλεπικοινωνιών, "ΟΤΕ". Σύμφωνα με τις αποφάσεις, εντοπίστηκαν παραβιάσεις του άρθρου 5, το οποίο αναφέρεται στην αρχή της

ακρίβειας και του άρθρου 21 που δίνει το δικαίωμα ένστασης του υποκειμένου σε επεξεργασία των προσωπικών του δεδομένων (Anon., 2019). Η εποπτική αρχή έλαβε διάφορες καταγγελίες από συνδρομητές του ΟΤΕ, οι οποίες είχαν λάβει κλήσεις από τρίτους για σκοπούς μάρκετινγκ, αν και έχουν εγγραφεί στο μητρώο της μη τηλεφωνικής εξυπηρέτησης του ΟΤΕ σύμφωνα με το άρθρο 11 του ελληνικού νόμου 3471/2006. Επίσης, ορισμένοι ιδιώτες κατήγγειλαν ότι δεν ήταν σε θέση να καταργήσουν την εγγραφή τους από τη λήψη διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου. Παρ' όλα αυτά στις αποφάσεις σημειώθηκε ότι «η Αρχή δέχεται ότι το συμβάν δεν οφείλεται σε δόλο του υπευθύνου επεξεργασίας και ότι μόλις ο υπεύθυνος επεξεργασίας το πληροφορήθηκε από την Αρχή, ενήργησε για την επανόρθωση της παράβασης, συνεργαζόμενος μαζί της» (Vlachou, 2019).

9. Πρόστιμο ύψους 120.000 ευρώ – Οκτώβριος 2019

Στις 11 Οκτωβρίου, η νορβηγική αρχή προστασίας των προσωπικών δεδομένων επέβαλε διοικητικό πρόστιμο ύψους 120.000 ευρώ στον Δήμο του Όσλο, και πιο συγκεκριμένα, στον Οργανισμό Εκπαίδευσης, ως αποτέλεσμα της ανεπαρκούς ασφάλειας επεξεργασίας σε μία εφαρμογή για κινητά. Η εφαρμογή προοριζόταν για την επικοινωνία μεταξύ των υπαλλήλων του σχολείου, των γονέων και των μαθητών.

Το πρόστιμο εκδόθηκε επειδή ο δήμος δεν είχε εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει το επίπεδο ασφάλειας για την προστασία των δεδομένων. Αρχικά, η Αρχή Προστασίας Δεδομένων γνωστοποίησε την πρόθεσή της να επιβάλει πρόστιμο ύψους 200.000 ευρώ ως απάντηση στις ανωτέρω διαπιστώσεις. Ωστόσο, το τελικό ποσό μειώθηκε σε 120.000 ευρώ, δεδομένου ότι υπήρχαν ελαφρυντικά στοιχεία στην υπόθεση. Ο Δήμος του Όσλο δεν άσκησε έφεση κατά της απόφασης αλλά αντιθέτως εφάρμοσε μέτρα για τον περιορισμό των ζημιών μόλις έλαβε γνώση των ελλείψεων ασφαλείας, και επέδειξε προθυμία για επίλυση των ζητημάτων (Anon., 2019).

10. Πρόστιμο ύψους 18.000.000 ευρώ – Οκτώβριος 2019

Στις 29 Οκτωβρίου 2019 επιβλήθηκε πρόστιμο από την αυστριακή αρχή προστασίας δεδομένων (DSB) στην εθνική ταχυδρομική υπηρεσία Österreichische Post AG (ÖPAG) συνολικής αξίας 18.000.00000 ευρώ για παραβιάσεις του GDPR, σχετικές με προσωπικά δεδομένα πολιτικής φύσεως πελατών τις εταιρίας. Οι εν λόγω

πληροφορίες στη συνέχεια χρησιμοποιήθηκαν για να προσφέρουν σε πολιτικά κόμματα συγκεκριμένες επιλογές μάρκετινγκ για στοχευμένη διαφήμιση (Anon., 2019). Όταν ήρθε στο φως το συμβάν οδήγησε σε δημόσια κατακραυγή, ιδίως λόγω του γεγονότος ότι τα στοιχεία των πελατών του ταχυδρομείου αφορούσαν μεγάλο αριθμό αυστριακών νοικοκυριών. Τα ειδησεογραφικά πρακτορεία ανέφεραν ότι 2,2 εκατομμύρια από αυτά τα σύνολα δεδομένων περιελάμβαναν επικριτικές πληροφορίες για ατομικές πολιτικές στάσεις. Ο Διευθυντής της Post CEO Pölzl ανακοίνωσε αμέσως ότι τα δεδομένα θα διαγραφούν. Εν μέσω της δημόσιας οργής, η DSB ξεκίνησε έρευνα, η οποία μετά από επίσημες διοικητικές διαδικασίες, συμπεριλαμβανομένης ακρόασης, είχε ως αποτέλεσμα το πρόστιμο που έχει πλέον δημοσιοποιηθεί (Panic, 2019).

11. Πρόστιμο ύψους 14.500.000 ευρώ – Νοέμβριος 2019

Το υψηλότερο πρόστιμο που έχει επιβάλει μέχρι σήμερα το γερμανικό GDPR αφορά την κτηματομεσιτική εταιρεία Deutsche Wohnen SE και αγγίζει το ποσό των 14,5 εκατ. Ευρώ (Anon., 2019). Η εν λόγω εταιρία δεν κατόρθωσε να θεσπίσει μία ορθή διαδικασία διατήρησης και διαγραφής των δεδομένων προσωπικού χαρακτήρα των ενοικιαστών και συνεπώς κατηγορήθηκε για παράβαση των υποχρεώσεων διαγραφής, βάση του άρθρου 25 παράγραφος 1 του GDPR. Παρά τα νέα μέτρα που έλαβε η εταιρία μετά από επιτόπιο έλεγχο το 2017, όπου διαπιστώθηκε η μη συμμόρφωση με τις υποχρεώσεις του Γενικού Κανονισμού, η εποπτική αρχή αποκάλυψε, κατά τη διάρκεια του δεύτερου ελέγχου της το 2019, ότι τα μέτρα αυτά δεν είχαν οδηγήσει στη δημιουργία αξιόπιστου συστήματος αρχειοθέτησης. Ο επικεφαλής της γερμανικής αρχής προστασίας δεδομένων του Βερολίνου ανακοίνωσε ορισμένες λεπτομέρειες σε συνέντευξή του. Συγκεκριμένα, ανέφερε ότι η Deutsche Wohnen θα μπορούσε εύκολα να συμμορφωθεί εφαρμόζοντας ένα σύστημα αρχειοθέτησης, το οποίο να διαχωρίζει τα δεδομένα με διαφορετικές περιόδους διατήρησης, επιτρέποντας έτσι διαφοροποιημένες περιόδους διαγραφής, καθώς τέτοιες λύσεις διατίθενται στο εμπόριο. Ωστόσο, η απόφαση του DPA του Βερολίνου δεν έχει ακόμη ολοκληρωθεί (Christoph Ritzer & Natalia Filkina, 2019).

12. Πρόστιμο ύψους 9.550.000 ευρώ – Δεκέμβριος 2019 (Telecom GmbH)

Στις 9 Δεκεμβρίου 2019, η γερμανική ομοσπονδιακή εποπτική αρχή προστασίας δεδομένων (BfDI) επέβαλε πρόστιμο 9,55 εκατ. ευρώ στην εταιρεία τηλεπικοινωνιών 1&1 Telecom GmbH. Η BfDI διαπίστωσε ότι οι διαδικασίες ελέγχου ταυτότητας που χρησιμοποιούνται από τη γραμμή βοήθειας του πελάτη ήταν ανεπαρκείς και δεν πληρούσαν τις απαιτήσεις του άρθρου 32 του GDPR. Η επιτροπή προστασίας δεδομένων της Γερμανίας ανέφερε ότι οποιοσδήποτε τηλεφωνούσε στην 1&1 Telecom GmbH μπορούσε να λάβει εκτενείς προσωπικές πληροφορίες για κάποιον άλλο μόνο αναφέροντας το όνομα και την ημερομηνία γέννησής του. Ωστόσο η εταιρεία ανακοίνωσε ότι θα αμφισβητήσει την απόφαση, υποστηρίζοντας ότι το μέγεθος του προστίμου είναι δυσανάλογο (Kelion, 2019). Σχετικά με το θέμα, ο Ομοσπονδιακός Επίτροπος Ulrich Kelber είπε: «Η προστασία των δεδομένων σημαίνει προστασία των θεμελιωδών δικαιωμάτων. Τα επιβαλλόμενα πρόστιμα αποτελούν σαφή ένδειξη ότι θα επιβάλουμε αυτήν την προστασία των θεμελιωδών δικαιωμάτων. Ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) μας δίνει την ευκαιρία να τιμωρήσουμε αποφασιστικά τις περιπτώσεις όπου εντοπίζεται ανεπάρκεια της προστασίας αυτής. Έτσι, εφαρμόζουμε τις αντίστοιχες εξουσίες λαμβάνοντας ταυτόχρονα υπόψη την απαιτούμενη αναλογικότητα» (Anon., 2019).

4.6 Έρευνες για την συμμόρφωση των επιχειρήσεων με το GDPR

Ήδη πριν από την δημοσίευση του Γενικού Κανονισμού και την υποχρεωτική εφαρμογή του στις 25 Μαΐου του 2018, ξεκίνησαν να διεξάγονται έρευνες σχετικά με την ετοιμότητα και την ικανότητα συμμόρφωσης των επιχειρήσεων με τις απαιτήσεις του GDPR. Παρόμοιες έρευνες διεξήχθησαν και στον ελληνικό επιχειρηματικό κόσμο. Παρακάτω παρουσιάζονται τα αποτελέσματα δύο ερευνών από τα οποία προκύπτει το κοινό συμπέρασμα ότι απαιτείται επιπλέον προσπάθεια από τις ελληνικές επιχειρήσεις προκειμένου να συμμορφωθούν πλήρως με τις απαιτήσεις του GDPR.

4.6.1 Η Έρευνα της ICAP

Η συγκεκριμένη αποτελεί πρωτογενή έρευνα που πραγματοποιήθηκε τον Δεκέμβριο του 2017, δηλαδή μόλις λίγους μήνες πριν την καθολική εφαρμογή του GDPR. Τα συμπεράσματα προέκυψαν μέσω ηλεκτρονικού ερωτηματολογίου που στάλθηκε σε 210 επιχειρήσεις και δεν αποτέλεσαν αισιόδοξο μήνυμα για την ετοιμότητα των επιχειρήσεων (ICAP, 2019):

- Σημαντικό ποσοστό ίσο με το 25% απάντησε ότι δεν γνωρίζει τον νέο Κανονισμό. Το 35% των επιχειρήσεων αυτών απασχολούν αριθμό εργαζομένων μικρότερο από 100 άτομα.
- Το 22% απάντησε ότι δεν γνωρίζει ακόμα τον ορισμό των προσωπικών δεδομένων. Το 32% των επιχειρήσεων αυτών ανήκουν στον Τουριστικό Κλάδο.
- Το 72% δήλωσε ότι επεξεργάζεται προσωπικά δεδομένα εκτός από αυτά των εργαζομένων της, όπως για παράδειγμα πελατών ή συνεργατών τους.
- Αξιοσημείωτο είναι το γεγονός ότι περίπου το 20% απάντησε πως δεν συμμορφώνεται με τον Κανονισμό ενώ σχεδόν το 58% συμμορφώνεται μερικώς, ειδικά όταν πρόκειται για έρευνα που διεξήχθη λίγο πριν την υποχρεωτική εφαρμογή του. Το μεγαλύτερο ποσοστό για ακόμη μια φορά παρουσιάστηκε σε επιχειρήσεις με λιγότερο από 100 εργαζόμενους.
- Εξίσου μεγάλο είναι και το ποσοστό των επιχειρήσεων που χαρακτήρισαν το επίπεδο των συστημάτων ασφαλείας τους ως μέτριο ή ανεπαρκές (31%). Ο τουρισμός κατέχει και σε αυτή την ερώτηση την πρώτη θέση με ποσοστό 40%.
- Με βάση την έρευνα, δεν έχει γίνει ξεκάθαρος ο ρόλος του Υπεύθυνου Προστασίας Δεδομένων καθώς 1 στις 2 επιχειρήσεις δεν γνωρίζει εάν πρέπει να ορίσει DPO και ιδιαίτερα όταν πρόκειται για μικρότερες επιχειρήσεις με αριθμό εργαζομένων κάτω των 100 ατόμων. Συνεπώς απαιτείται καλύτερη ενημέρωση επί του συγκεκριμένου θέματος.

4.6.2 Η Έρευνα του ΣΕΒ

Το δείγμα της έρευνας αποτέλεσαν 35 επιχειρήσεις, αποκλειστικά μέλη του ΣΕΒ και η διάρκειά της ορίστηκε από 13 έως 23 Φεβρουαρίου 2018. Πρόκειται για περιορισμένης

έκτασης έρευνα και τα αποτελέσματα της παρουσιάζονται συνοπτικά παρακάτω (Ομάδας Εργασίας του ΣΕΒ, 2018) :

- Δραματικά μεγάλο είναι το ποσοστό (8 στις 10) των επιχειρήσεων με μέτριο ή χαμηλό βαθμό ετοιμότητας ως προς τη συμμόρφωσή τους με τις απαιτήσεις του GDPR. Συνεπώς, είναι εμφανές ότι δεν έχουν λάβει ακόμη όλα τα απαραίτητα μέτρα.
- Περισσότερες από τις μισές επιχειρήσεις δήλωσαν ότι συμβουλεύονται παράλληλα και ειδικούς προκειμένου να αντιμετωπίσουν τα ζητήματα που προκύπτουν από την υποχρεωτική εφαρμογή του Κανονισμού. Αυτό υποδηλώνει μια «ανασφάλεια» από την μεριά των επιχειρήσεων να διαχειριστούν τα θέματα του GDPR.
- Περίπου το 77% του δείγματος θεωρεί ότι το κόστος συμμόρφωσης μιας επιχείρησης είναι μικρότερο από 40.000€, ενώ αντιθέτως οι εταιρίες που εκτίμησαν το κόστος αυτό μεγαλύτερο από το ποσό αυτό, παρουσίαζαν κύκλο εργασιών μεγαλύτερο των 100.000€. Το γεγονός αυτό αποκαλύπτει πως οι επιχειρήσεις συνδέουν το μέγεθος της εταιρίας με το κόστος συμμόρφωσης.
- Αισιόδοξο μήνυμα αποτελεί το υψηλό ποσοστό (88,6%) των συμμετεχόντων που πιστεύουν στην αναγκαιότητα της απαραίτητης εκπαίδευσης εντός των οργανισμών και μάλιστα έχουν προβεί σε τέτοιες ενέργειες.
- Τέλος, έχει καταστεί αντιληπτό από τις μισές τουλάχιστον εταιρίες ότι η συμμόρφωση με τις αρχές του GDPR αποτελεί μια σύνθετη διαδικασία που απαιτεί ποικίλες ενέργειες σε διάφορους τομείς μιας επιχείρησης όπως στο πληροφοριακό της σύστημα, στην ενημέρωση-εκπαίδευση του προσωπικού της και στην γενικότερη κουλτούρα και πολιτική της.

4.6.3 Συνοπτικά συμπεράσματα

Είναι εμφανές ότι το κύριο συμπέρασμα που προκύπτει και από τις δύο παραπάνω έρευνες είναι ότι ελάχιστες επιχειρήσεις στον ελληνικό χώρο είναι κατάλληλα προετοιμασμένες να υποδεχτούν το GDPR και μαζί μ' αυτό, τις αλλαγές που θα επιφέρει. Σίγουρα αποτελεί κάτι πρωτόγνωρο για πολλές από αυτές και ίσως να υπάρχει δυσκολία στην κατανόηση από μεριάς τους τόσο των απαιτήσεων όσο και των εννοιών που εισάγει ο νέος αυτός

Κανονισμός, όπως για παράδειγμα, ο ορισμός ενός Υπεύθυνου Προστασίας Δεδομένων (DPO).

Ανάλογα πορίσματα παρουσίασαν και έρευνες, όπως αυτή της Ernest & Young το 2018, σε παγκόσμιο επίπεδο. Πιο συγκεκριμένα, την εποχή που πραγματοποιήθηκε η έρευνα, μόνο το 33% των ερωτηθέντων είχε ένα σχέδιο για να αντιμετωπίσει τη συμμόρφωση με το GDPR ενώ παράλληλα το 39% των ερωτηθέντων ανέφερε ότι δεν είναι καθόλου εξοικειωμένοι με το GDPR. Τέλος, μόλις ένα 17% δήλωσε ότι έχει γνώση για τον Γενικό Κανονισμό αλλά δεν έχει προχωρήσει σε κάποια ενέργεια σχετική με αυτόν. Αξίζει να σημειωθεί ότι όσο αφορά τις εταιρείες που είχαν θέσει σε εφαρμογή ένα σχέδιο συμμόρφωσης, οι ευρωπαίοι παρουσίασαν υψηλότερα ποσοστά της τάξεως του 60%, θέτοντας ένα προβάδισμα σε σχέση με τις υπόλοιπες εταιρίες ανά τον κόσμο. (Ernest & Young, 2018)

Παρ’ όλα αυτά, τα αποτελέσματα τόσο της έρευνας της ICAP όσο και του ΣΕΒ αναφέρονται χρονικά στο 2018, και μάλιστα λίγους μήνες πριν την καθολική εφαρμογή του Γενικού Κανονισμού Προστασίας των Δεδομένων. Συνεπώς, αποτύπωσαν εκείνη τη συγκεκριμένη χρονική περίοδο πως αντιμετώπιζε ο επιχειρηματικός κόσμος τον ερχομό του GDPR. Σχεδόν δύο χρόνια μετά, τα πράγματα έχουν εμφανώς αλλάξει, καθώς ο νέος αυτός Κανονισμός αποτελεί πλέον κομμάτι της καθημερινότητας των επιχειρήσεων.

ΚΕΦΑΛΑΙΟ 5

ΠΑΡΟΥΣΙΑΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ

5.1 Περιγραφικά στατιστικά του Δείγματος

Στο δεύτερο και τελευταίο μέρος της παρούσας διπλωματικής παρουσιάζονται τα αποτελέσματα της ποσοτικής έρευνας που διενεργήθηκε μέσω ερωτηματολογίου. Το θέμα της έρευνας είναι η εφαρμογή του νέου Ευρωπαϊκού Κανονισμού (5419/16) στα λογιστικά γραφεία του νομού Θεσσαλονίκης. Σε αυτό το κεφάλαιο παρατίθεται η μεθοδολογία που ακολουθήθηκε προκειμένου να πραγματοποιηθεί η ποσοτική έρευνα.

5.1.1. Δειγματοληπτικό πλαίσιο

Το δείγμα της έρευνας αποτελούν λογιστικά γραφεία τα οποία εδρεύουν τόσο στην Θεσσαλονίκη όσο και στην ευρύτερη περιοχή του νομού Θεσσαλονίκης. Πηγή άντλησης πληροφοριών για τα στοιχεία επικοινωνίας των γραφείων και κυρίως των επαγγελματικών τους διευθύνσεων ηλεκτρονικού ταχυδρομείου (e-mails), προκειμένου να τους αποσταλεί το ερωτηματολόγιο, αποτέλεσαν οι σελίδες www.xo.gr και www.vrisko.gr. Οι ιστοσελίδες αυτές παρέχουν υπηρεσίες εύρεσης πληροφοριών, τις οποίες οι ίδιες οι επιχειρήσεις επιθυμούν να κοινοποιήσουν στο διαδίκτυο και περιλαμβάνουν συνήθως την επωνυμία της επιχείρησης, την διεύθυνσή της, τα τηλέφωνα επικοινωνίας, τα emails και το site της εταιρίας, εφόσον διαθέτει. Μέσω των παραπάνω πηγών εντοπίστηκαν 89 λογιστικά γραφεία που δραστηριοποιούνται στο νομό Θεσσαλονίκης και στη συνέχεια ακολούθησε η αποστολή του ερωτηματολογίου.

5.1.2. Σχεδιασμός ερωτηματολογίου

Η μελέτη της σχετικής βιβλιογραφίας αποτέλεσε τη βάση για να δημιουργηθεί το ερωτηματολόγιο, το οποίο σχεδιάστηκε με τη χρήση Google Forms. Το εργαλείο αυτό αποτελεί συχνή επιλογή για τη σύνταξη ηλεκτρονικών ερωτηματολογίων, παρέχοντας διάφορα πλεονεκτήματα, όπως η εξοικονόμηση χρόνου και χρήματος, η μαζική αποστολή τους σε μεγάλο αριθμό ατόμων και η εύκολη επεξεργασία τους μετά το πέρας της συλλογής δεδομένων μέσω άλλων εφαρμογών. Σχετικά με την δομή του, το πρώτο μέρος περιλαμβάνει δώδεκα ερωτήσεις κλειστού τύπου που αποτελούν βασικές ερωτήσεις που σχετίζονται με τα ερευνητικά ερωτήματα. Επιλέχθηκαν ερωτήσεις διαβαθμισμένης κλίμακας ή αλλιώς κλίμακας Likert (Καθόλου, Λίγο, Μέτρια, Πολύ, Πάρα πολύ) καθώς και ερωτήσεις πολλαπλών επιλογών με μία ή περισσότερες απαντήσεις. Στο δεύτερο μέρος παρατίθενται τέσσερις δημογραφικές ερωτήσεις. Αξίζει να σημειωθεί ότι όλες οι ερωτήσεις είχαν υποχρεωτικό χαρακτήρα. Συνεπώς, δεν υπήρξαν αναπάντητα ερωτήματα.

5.1.3. Συλλογή δεδομένων

Η αποστολή του ερωτηματολογίου, όπως προαναφέρθηκε, πραγματοποιήθηκε με την προώθησή του μέσω ηλεκτρονικού ταχυδρομείου στα λογιστικά γραφεία και η διάρκεια που παρέμεινε ανοιχτή η Φόρμα για την υποβολή απαντήσεων ήταν περίπου δύο μήνες. Συνολικά συγκεντρώθηκαν απαντήσεις από 34 λογιστικά γραφεία (ποσοστό συμμετοχής 38,2%). Η έρευνα διεξήχθη ανώνυμα και με απόλυτη εμπιστευτικότητα απέναντι στις πληροφορίες των συμμετεχόντων.

ΚΕΦΑΛΑΙΟ 6

ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΕΡΜΗΝΕΙΑ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

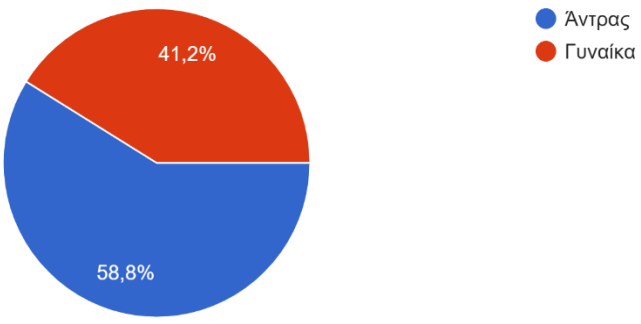
6.1 Περιγραφή Δείγματος

6.1.1 Δημογραφικά δεδομένα

Στα παρακάτω 1, 2, 3 και 4 διαγράμματα παρουσιάζεται το δείγμα ανάλογα με το φύλο, την ηλικία, την ιδιότητα των συμμετεχόντων στα λογιστικά γραφεία και τα έτη λειτουργίας αυτών.

Φύλο

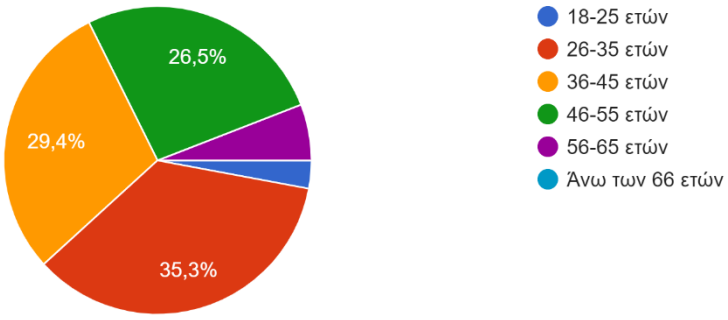
Από τον συνολικό αριθμό των ερωτηθέντων, ήτοι 34 άτομα, το 58,8% (n=20) είναι άντρες και το 41,2% (n=14) είναι γυναίκες.



Διάγραμμα 1: Περιγραφή στατιστικών δείγματος ανά φύλο

Ηλικία

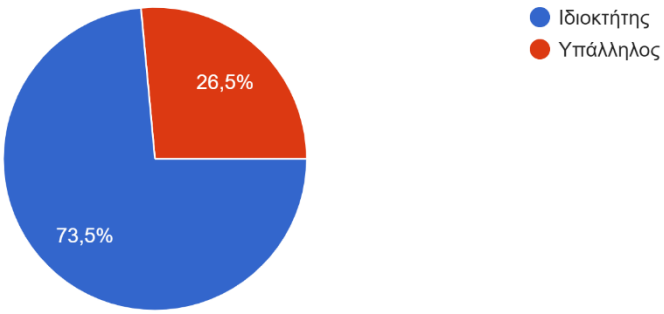
Σχετικά με την ηλικιακή ομάδα που ανήκουν οι συμμετέχοντες, στην έρευνα έχουμε τα εξής: το 2,9% (n=1) είναι ηλικίας 18-25 ετών, το 35,3% (n=12) είναι 26-35 ετών, το 29,4% (n=10) είναι 36-45 ετών, το 26,5% (n=9) είναι 46-55 ετών, και το 5,9% (n=2) είναι 56-65. Δεν υπήρξε συμμετοχή ατόμων ηλικίας άνω των 66 ετών.



Διάγραμμα 2: Περιγραφή στατιστικών δείγματος ανά ηλικία

Ιδιότητα στην επιχείρηση

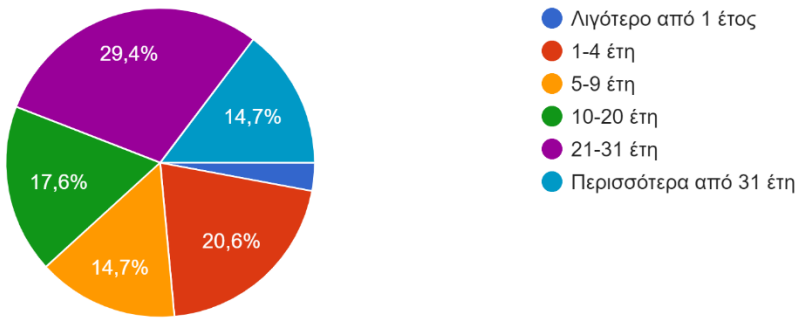
Όσον αφορά την ιδιότητα των ερωτηθέντων στην επιχείρηση, το 73,5% (n=25) είναι ιδιοκτήτες των λογιστικών γραφείων ενώ το 26,5% (n=9) είναι εργαζόμενοι στην επιχείρηση.



Διάγραμμα 3: Περιγραφή στατιστικών δείγματος ανά ιδιότητα στην επιχείρηση

Έτη λειτουργίας της επιχείρησης

Τα έτη λειτουργίας των λογιστικών γραφείων απεικονίζονται στο παρακάτω διάγραμμα. Μόλις το 2,9% (n=1) λειτουργεί λιγότερο από ένα έτος, το 20,6% (n=7) από 1 έως 4 έτη, το 14,7% (n=5) από 5 έως 9 έτη, το 17,6% (n=6) από 10 έως 20 έτη, το 29,4% (n=10) από 21 έως 31 έτη και το 14,7% (n=5) περισσότερα από 31 έτη.



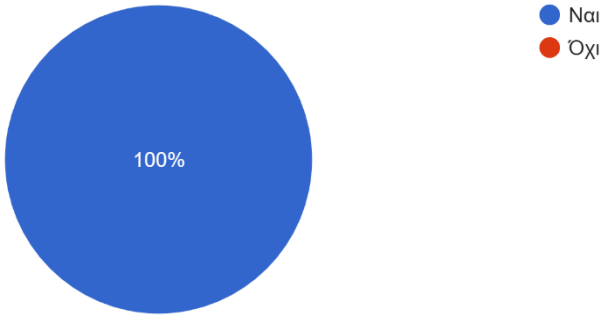
Διάγραμμα 4: Περιγραφή στατιστικών δείγματος ανά έτη λειτουργίας της επιχείρηση

6.2 Ανάλυση εμπειρικών αποτελεσμάτων

Στα διαγράμματα που ακολουθούν παρουσιάζονται τα αποτελέσματα των απαντήσεων που δόθηκαν από τους συμμετέχοντες στο ερωτηματολόγιο της έρευνας.

Ερώτηση 1η

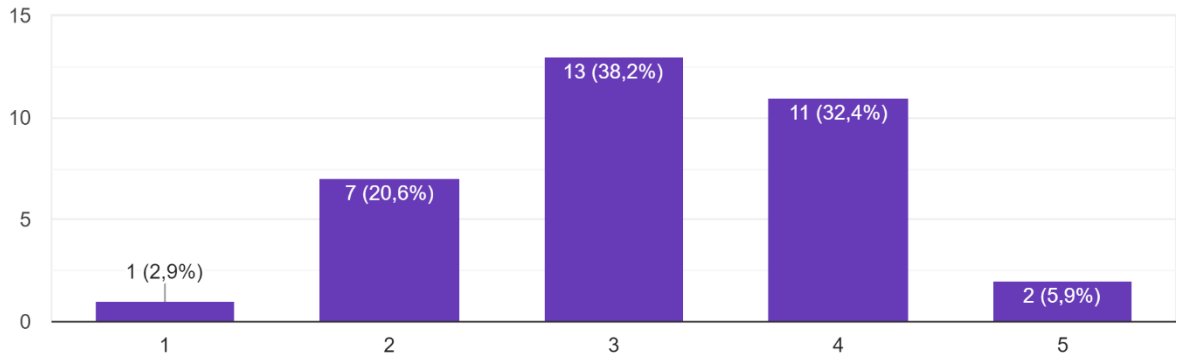
Στην πρώτη ερώτηση οι συμμετέχοντες έπρεπε να απαντήσουν για το αν είναι ενημερωμένοι σχετικά με το νέο Ευρωπαϊκό Κανονισμό (5419/16), που αφορά την προστασία προσωπικών δεδομένων και τέθηκε σε εφαρμογή στις 25 Μαΐου 2018. Το 100% (n=34) των ερωτηθέντων απάντησε καταφατικά στην συγκεκριμένη ερώτηση. Συνεπώς, δεν υπήρξε κανένας που να μην έχει ενημερωθεί για το νέο αυτό Κανονισμό.



Διάγραμμα 5: Περιγραφή στατιστικών δείγματος 1ης Ερώτησης

Ερώτηση 2η

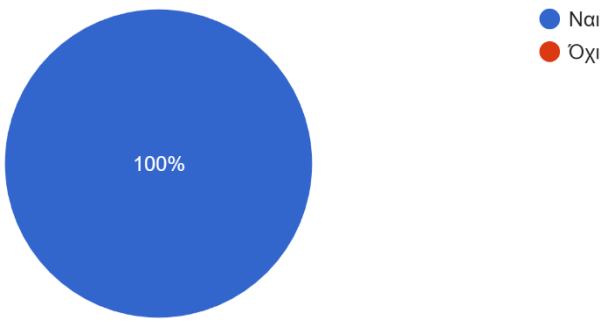
Στην δεύτερη ερώτηση οι συμμετέχοντες εξέφρασαν τη γνώμη τους σχετικά με το πόσο έχει επηρεαστεί το επάγγελμα του λογιστή μετά από τις αλλαγές που έχει επιφέρει η υποχρεωτική εφαρμογή του νέου Ευρωπαϊκού Κανονισμού (5419/16), που αφορά την προστασία προσωπικών δεδομένων. Τα αποτελέσματα είναι τα εξής: Καθόλου μόλις το 2,9% (n=1), λίγο το 20,6% (n=7), μέτρια το 38,2% (n=13), πολύ το 32,4% (n=11) και πάρα πολύ το 5,9% (n=2).



Διάγραμμα 6: Περιγραφή στατιστικών δείγματος 2ης Ερώτησης

Ερώτηση 3η

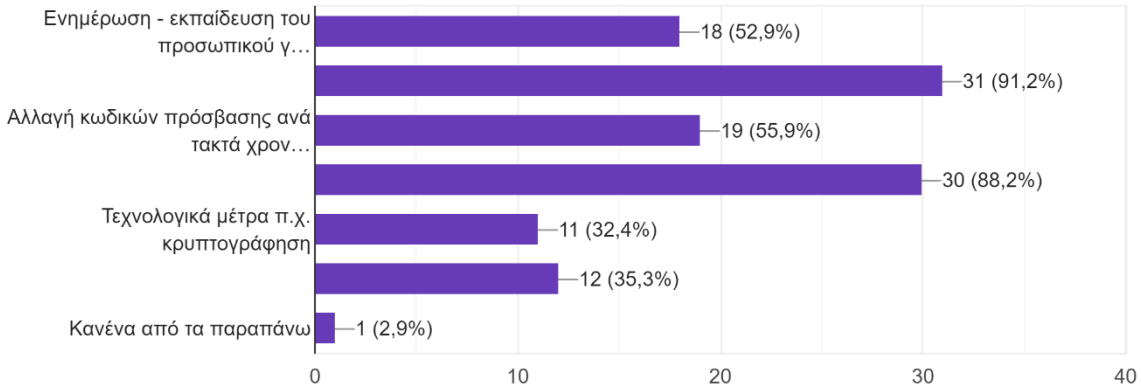
Στην τρίτη ερώτηση οι συμμετέχοντες κλήθηκαν να δηλώσουν εάν έχουν λάβει μέτρα προκειμένου να συμμορφωθούν με τις με τις διατάξεις του νέου Ευρωπαϊκού Κανονισμού (5419/16), που αφορά την προστασία προσωπικών δεδομένων. Για ακόμη μία φορά, το 100% (n=34) απάντησε θετικά στην συγκεκριμένη ερώτηση. Επομένως δεν υπήρξε κάποιος που να μην έχει λάβει έστω και ένα μέτρο.



Διάγραμμα 7: Περιγραφή στατιστικών δείγματος 3ης Ερώτησης

Ερώτηση 4η

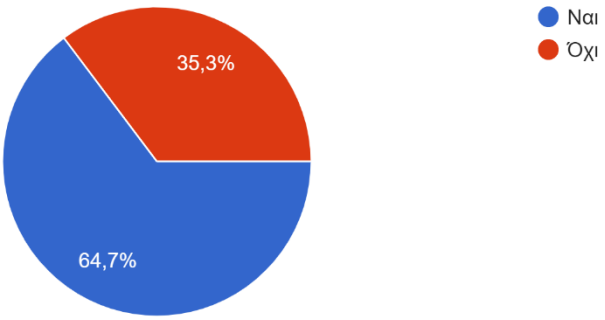
Στην τέταρτη ερώτηση οι συμμετέχοντες έπρεπε να επιλέξουν μεταξύ ορισμένων μέτρων που εφαρμόζουν προκειμένου να προστατεύσουν τα προσωπικά δεδομένα που διαχειρίζονται ως λογιστικό γραφείο. Οι απαντήσεις που λάβαμε είναι οι ακόλουθες: Το 52,9% (n=18) επιλέγει την ενημέρωση - εκπαίδευση του προσωπικού για ευαισθητοποίηση σε θέματα ασφαλείας, το 91,2% (n=31) εγκαθιστά και χρησιμοποιεί ενημερωμένα προγράμματα antivirus, firewalls κλπ, το 55,9% (n=19) αλλάζει κωδικούς πρόσβασης ανά τακτά χρονικά διαστήματα, το 88,2% (n=30) εκτελεί Back up της βάσης δεδομένων ανά τακτά χρονικά διαστήματα, το 32,4% (n=11) χρησιμοποιεί τεχνολογικά μέτρα όπως η κρυπτογράφηση, το 35,3% (n=12) των λογιστικών γραφείων έχει υιοθετήσει μία πολιτική για την ασφάλεια και αντιμετώπιση των περιστατικών απώλειας προσωπικών δεδομένων ενώ μόνο το 2,9% (n=1) δεν έχει επιλέξει κανένα από τα παραπάνω μέτρα.



Διάγραμμα 8: Περιγραφή στατιστικών δείγματος 4ης Ερώτησης

Ερώτηση 5η

Στην πέμπτη ερώτηση οι συμμετέχοντες απάντησαν με «Ναι» ή «Όχι» για το αν έχουν έγγραφη συγκατάθεση των πελατών τους που τους επιτρέπει να διαχειρίζονται τα προσωπικά τους δεδομένα. Το 64,7% (n=22) απάντησαν θετικά ενώ το 35,3% (n=12) απάντησαν αρνητικά.



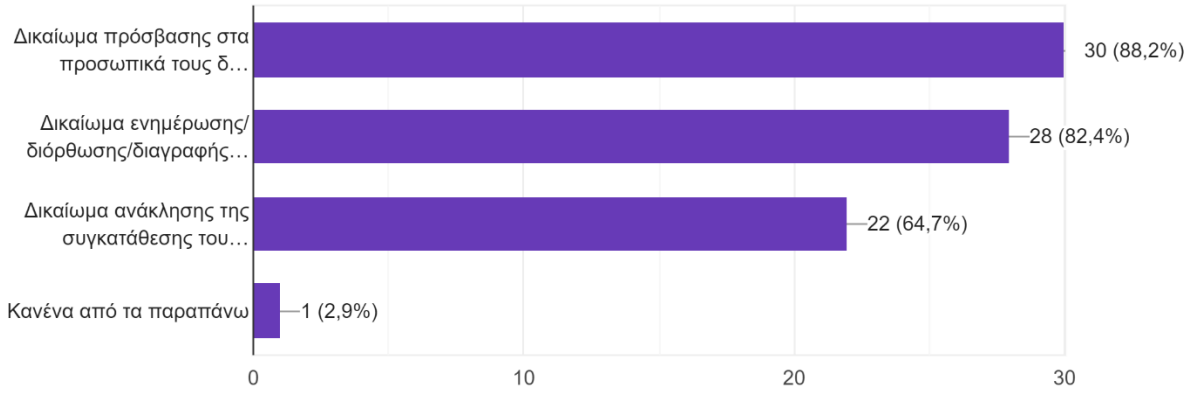
Διάγραμμα 9: Περιγραφή στατιστικών δείγματος 5ης Ερώτησης

Ερώτηση 6η

Στην έκτη ερώτηση οι συμμετέχοντες έπρεπε να διαλέξουν ποια δικαιώματα παρέχουν στους πελάτες τους από τη στιγμή που διατηρούν τα προσωπικά τους δεδομένα. Οι επιλογές που είχαν ήταν οι παρακάτω:

1. Δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα
2. Δικαίωμα ενημέρωσης/διόρθωσης/διαγραφής των προσωπικών τους δεδομένων
3. Δικαίωμα ανάκλησης της συγκατάθεσης τους για διαχείριση των προσωπικών τους δεδομένων
4. Κανένα από τα παραπάνω

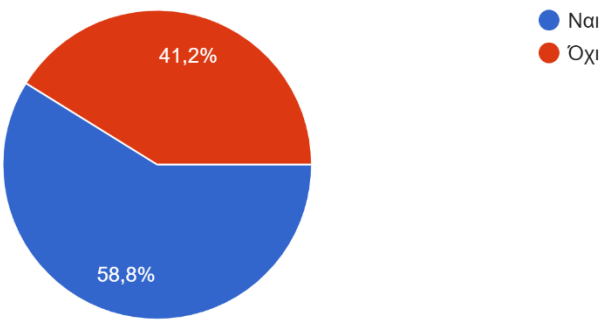
Τα ποσοστά που συλλέξαμε είναι: 88,2% (n=30) για την πρώτη επιλογή, 82,4% (n=28) για την δεύτερη επιλογή, 64,7% (n=22) για την τρίτη επιλογή και μόνο το 2,9% (n=1) δεν δίνει καμία από τις παραπάνω επιλογές.



Διάγραμμα 10: Περιγραφή στατιστικών δείγματος 6ης Ερώτησης

Ερώτηση 7η

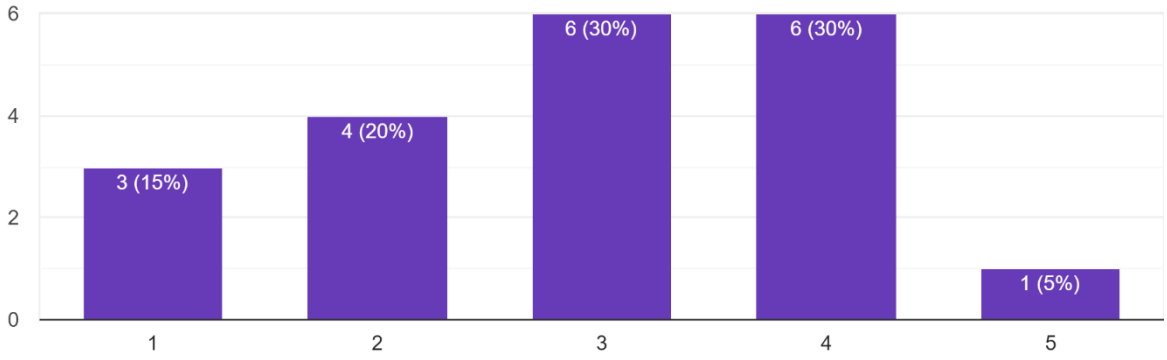
Στην έβδομη ερώτηση ζητήσαμε από τους ερωτηθέντες να μας πληροφορήσουν για το αν κάνουν ή όχι χρήση υπηρεσιών cloud (π.χ. Google Drive, Dropbox, WeTransfer κλπ) στο λογιστικό τους γραφείο. Το 58,8% (n=20) δήλωσε ότι κάνει χρήση ανάλογων υπηρεσιών ενώ το 41,2% (n=14) απάντησε αρνητικά στην συγκεκριμένη ερώτηση.



Διάγραμμα 11: Περιγραφή στατιστικών δείγματος 7ης Ερώτησης

Ερώτηση 8η

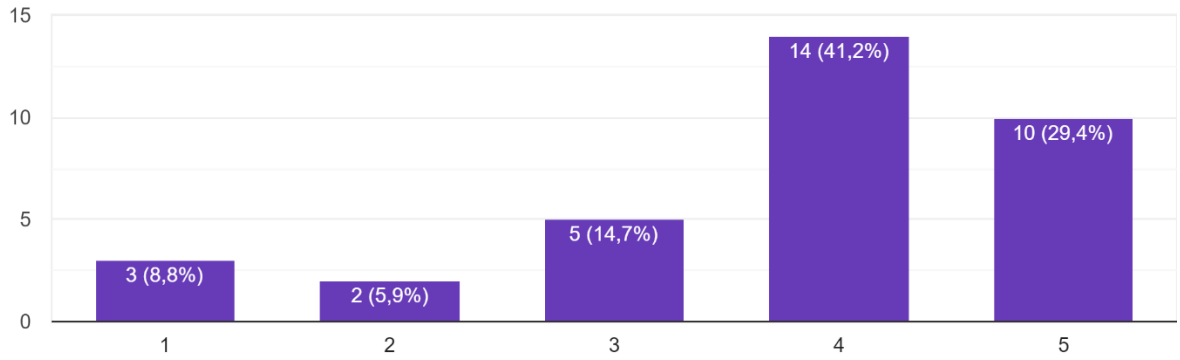
Στην όγδοη ερώτηση απάντησαν μόνο όσοι απάντησαν θετικά στην προηγούμενη ερώτηση (n=20), δηλώνοντας την άποψή τους για το αν η χρήση υπηρεσιών cloud τους καθιστά περισσότερο ευάλωτους απέναντι σε κινδύνους απώλειας ή διαρροής των προσωπικών δεδομένων που διαχειρίζονται ως λογιστικό γραφείο. Οι απαντήσεις που δόθηκαν ήταν οι εξής: Το 15% (n=3) δήλωσε Καθόλου, το 20% (n=4) Λίγο, το 30% (n=6) Μέτρια, το 30% (n=6) Πολύ και μόνο το 5% (n=1) δήλωσε Πάρα Πολύ.



Διάγραμμα 12: Περιγραφή στατιστικών δείγματος 8ης Ερώτησης

Ερώτηση 9η

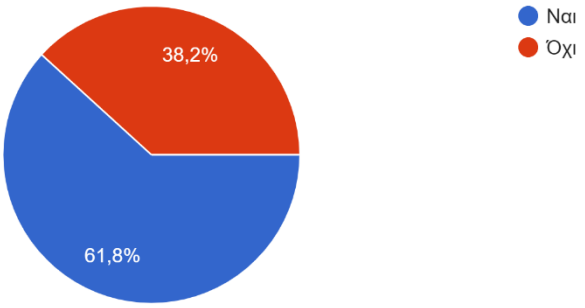
Στην ένατη ερώτηση οι συμμετέχοντες ερωτήθηκαν σε ποιο βαθμό πιστεύουν ότι ένα περιστατικό παραβίασης της ασφάλειας των προσωπικών δεδομένων θα έχει επιπτώσεις (π.χ. οικονομικές, φήμης κλπ) για το λογιστικό τους γραφείο. Το 8,8% (n=3) πιστεύει ότι κάτι τέτοιο δεν θα έχει καθόλου επιπτώσεις γι' αυτούς, το 5,9% (n=2) θεωρεί θα επηρεάσει λίγο, το 14,7% (n=5) θεωρεί μέτρια, το 41,2% (n=14) θεωρεί πολύ και το 29,4% (n=10) θεωρεί πάρα πολύ.



Διάγραμμα 13: Περιγραφή στατιστικών δείγματος 9ης Ερώτησης

Ερώτηση 10η

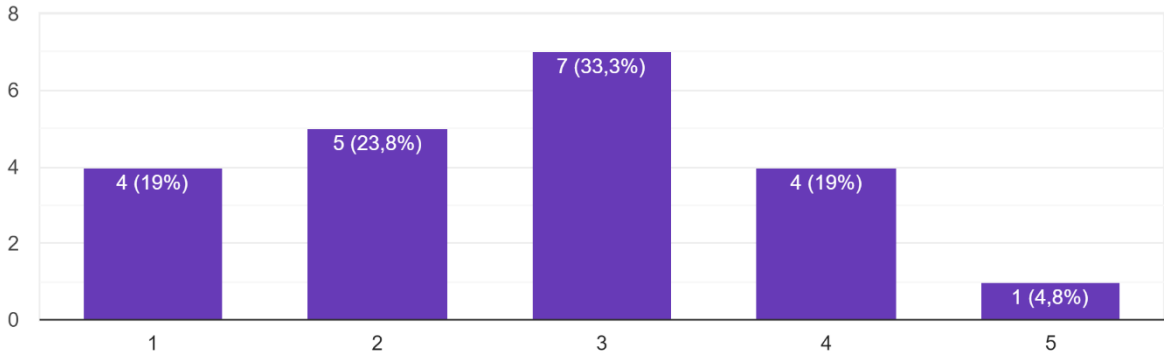
Η δέκατη ερώτηση ζητούσε από τους συμμετέχοντες να απαντήσουν είτε «Ναι» εφόσον γνωρίζουν την ύπαρξη ασφαλιστήριων συμβολαίων κάλυψης από ηλεκτρονικούς και διαδικτυακούς κινδύνους (cyber insurance), είτε «Όχι» εάν δεν έχουν τέτοια ενημέρωση. Τα αποτελέσματα είναι: 61,8% (n=21) επέλεξαν «Ναι» και 38,2% επέλεξαν «Όχι».



Διάγραμμα 14: Περιγραφή στατιστικών δείγματος 10ης Ερώτησης

Ερώτηση 11η

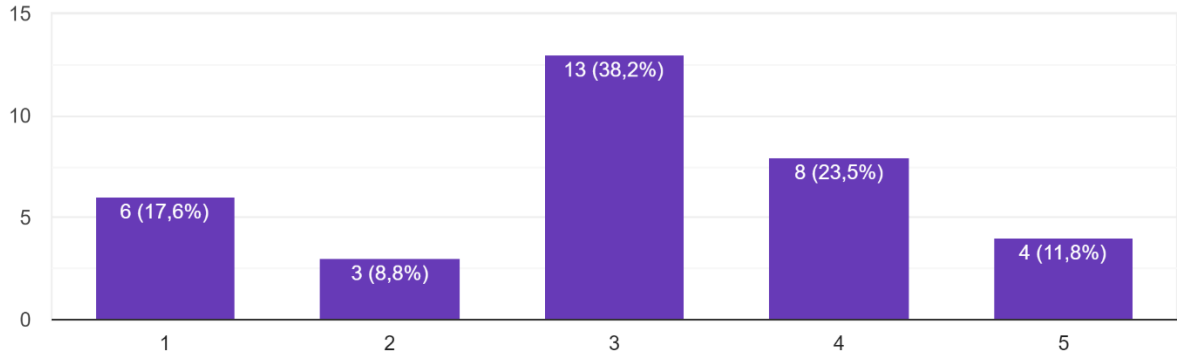
Η ενδέκατη ερώτηση απευθυνόταν μόνο σε όσους απάντησαν θετικά στην προηγούμενη ερώτηση (n=21) και ερωτήθηκαν κατά πόσο είναι διατεθειμένοι να προβούν στην αγορά ενός ασφαλιστήριου συμβολαίου προκειμένου να καλύψουν τις χρηματοοικονομικές τους επιπτώσεις. Ξεκινώντας από την χαμηλότερη κλίμακα, το 19% (n=4) δεν είναι καθόλου διατεθειμένοι να προβούν σε τέτοια αγορά, το 23,8% (n=5) είναι λίγο, το 33,3% (n=7) είναι μέτρια, το 19% (n=4) είναι πολύ και μόνο το 4,8% (n=1) είναι πάρα πολύ.



Διάγραμμα 15: Περιγραφή στατιστικών δείγματος 11ης Ερώτησης

Ερώτηση 12η

Η δωδέκατη και τελευταία ερώτηση του ερωτηματολογίου ζητούσε την άποψη των συμμετεχόντων σχετικά με τον βαθμό που θεωρούν ότι η εφαρμογή του νέου Ευρωπαϊκού Κανονισμού (5419/16) έχει ευεργετικά αποτελέσματα για την προστασία των προσωπικών δεδομένων που διαχειρίζεται το γραφείο τους. Με βάση την παρακάτω κλίμακα, η απάντηση «Καθόλου» συγκέντρωσε το 17,6% (n=6), η απάντηση «Λίγο» το 8,8% (n=3), η απάντηση «Μέτρια» το 38,2% (n=13), η απάντηση «Πολύ» το 23,5% (n=8) και η απάντηση «Πάρα πολύ» το 11,8% (n=4).



Διάγραμμα 16: Περιγραφή στατιστικών δείγματος 12ης Ερώτησης

ΚΕΦΑΛΑΙΟ 7

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

7.1 Συμπεράσματα

Το ερωτηματολόγιο της έρευνας σχεδιάστηκε ακολουθώντας μία νοητή σειρά προκειμένου να δοθούν απαντήσεις στα ερευνητικά ερωτήματα που τέθηκαν στο πρώτο κεφάλαιο της παρούσας διπλωματικής. Μετά την συλλογή και μελέτη των αποτελεσμάτων που προέκυψαν από τις απαντήσεις των συμμετεχόντων μπορούμε να εξάγουμε τα παρακάτω συμπεράσματα.

Ιδιαίτερα ενθαρρυντικό είναι το γεγονός ότι όλοι οι ερωτηθέντες έχουν ενημερωθεί για τον νέο Ευρωπαϊκό Κανονισμό (5419/16) που αφορά την προστασία προσωπικών δεδομένων και έχουν λάβει μέτρα προκειμένου να συμμορφωθούν με τις απαιτήσεις που αυτός ορίζει. Αυτό οφείλεται, κατά κύριο λόγο, στο ότι έχουν παρέλθει δύο ολόκληρα χρόνια από την υποχρεωτική εφαρμογή του Κανονισμού και μέσα σ αυτό το διάστημα είναι λογικό να έχει κινητοποιηθεί ο λογιστικός κλάδος, ο οποίος χρησιμοποιεί, κατά κόρον, προσωπικά δεδομένα.

Επίσης, διακρίνουμε ότι ο Κανονισμός έχει μια μέτρια προς μεγάλη επιρροή στο επάγγελμα του λογιστή, ενώ ελάχιστοι είναι αυτοί που θεωρούν ότι η επίδραση του είναι μηδενική. Όσο αφορά τα μέτρα, το μεγαλύτερο ποσοστό των λογιστικών γραφείων χρησιμοποιεί ενημερωμένα προγράμματα antivirus, firewalls κλπ, και εκτελεί back up της βάσης δεδομένων ανά τακτά χρονικά διαστήματα προκειμένου να αποφύγει ένα περιστατικό απώλειας δεδομένων. Επιπλέον, αρκετοί είναι αυτοί που έχουν λάβει ως μέτρο την αλλαγή κωδικών πρόσβασης ανά τακτά χρονικά διαστήματα και την ενημέρωση - εκπαίδευση του προσωπικού για ευαισθητοποίηση σε θέματα ασφαλείας. Μικρότερο ποσοστό επιλέγει μέτρα όπως η κρυπτογράφηση και η υιοθέτηση πολιτικής για την ασφάλεια και αντιμετώπιση των περιστατικών απώλειας προσωπικών δεδομένων.

Ωστόσο, περίπου ένας στους τρεις δεν έχει έγγραφη συγκατάθεση των πελατών του που του επιτρέπει να διαχειρίζεται προσωπικά του δεδομένα. Στη συγκεκριμένη ενέργεια

πιθανόν να μην δίνεται ιδιαίτερη βαρύτητα από τα λογιστικά γραφεία λόγω της οικειότητας που αναπτύσσουν με τους επί χρόνια πελάτες τους. Έτσι, οι λογιστές φτάνουν στο σημείο να θεωρούν ότι η συγκατάθεσή τους είναι αυτονόητη και δεν είναι απαραίτητο να τους δοθεί γραπτώς. Παράλληλα, χρειάζεται να αναφερθεί ότι η πλειοψηφία επιτρέπει στους πελάτες της να έχουν πρόσβαση στα δεδομένα τους και να τα διορθώσουν ή να τα διαγράψουν, παρέχοντας τους με αυτό τον τρόπο, τα βασικότερα δικαιώματα που ορίζονται στα άρθρα 16 – 18 του Κανονισμού.

Ένα ακόμη ζήτημα το οποίο ερευνήσαμε είναι εάν οι συμμετέχοντες νιώθουν ευάλωτοι απέναντι σε κινδύνους απώλειας ή διαρροής των προσωπικών δεδομένων που διαχειρίζονται εξαιτίας της χρήσης υπηρεσιών cloud όπως το Google Drive, το Dropbox κλπ. Τον ίδιο αριθμό απαντήσεων έλαβαν οι απαντήσεις «μέτρια» και «πολύ» ενώ δεν ήταν λίγοι αυτοί που απάντησαν ότι δεν αισθάνονται καμία απειλή μέσω της χρήσης τέτοιων υπηρεσιών, γεγονός που φανερώνει, ίσως, μια άγνοια κινδύνου από μεριάς τους. Παράλληλα, η συντριπτική πλειοψηφία συνδέει ένα περιστατικό παραβίασης της ασφάλειας των προσωπικών δεδομένων με αρνητικές συνέπειες, όπως οικονομικές ή απώλειας φήμης κ.α.

Τέλος, περισσότεροι από τους μισούς γνωρίζουν την ύπαρξη ασφαλιστήριων συμβολαίων κάλυψης από ηλεκτρονικούς και διαδικτυακούς κινδύνους (cyber insurance). Απεναντίας, είναι μικρό το ποσοστό που δήλωσε ότι θα προέβαινε στην αγορά ενός ασφαλιστήριου συμβολαίου προκειμένου να καλύψει τις χρηματοοικονομικές του επιπτώσεις. Η μέθοδος αυτή αποτελεί ένα νέο εργαλείο με το οποίο πολλοί δεν είναι εξοικειωμένοι και πιθανότατα είναι λίγο νωρίς για τα επαγγέλματα του λογιστικού κλάδου στην Ελλάδα να υποδεχτούν κάτι τέτοιο.

7.2 Περιορισμοί της έρευνας

Οι περιορισμοί που εντοπίστηκαν κατά την διεξαγωγή της έρευνας είναι οι ακόλουθοι:

1. Το ερωτηματολόγιο στάλθηκε μόνο σε λογιστικά γραφεία που βρίσκονται στον νομό Θεσσαλονίκης και η συλλογή των στοιχείων επικοινωνίας τους έγινε μέσω διαδικτυακών ιστότοπων που παρέχουν υπηρεσίες εύρεσης πληροφοριών.
2. Το ερωτηματολόγιο στάλθηκε σε 89 λογιστικά γραφεία, εκ των οποίων λάβαμε απαντήσεις από τα 34.

3. Η έρευνα διεξήχθη κατά τους μήνες υποβολής των φορολογικών δηλώσεων που αποτελεί περίοδο υψηλού φόρτου εργασίας για τα λογιστικά γραφεία.

7.3 Προτάσεις για περαιτέρω έρευνα

Με βάση την παρούσα έρευνα μπορούν να διερευνηθούν τα ίδια ερευνητικά ερωτήματα σε πανελλαδικό επίπεδο ώστε να υπάρξει μια συνολική εικόνα της εφαρμογής του Γενικού Κανονισμού στα λογιστικά γραφεία της χώρας. Επίσης, μπορεί να γίνει μια συγκριτική ανάλυση μεταξύ των λογιστικών γραφείων και των λογιστηρίων των επιχειρήσεων ως προς τον τρόπο συμμόρφωσης του καθενός με τις απαιτήσεις του GDPR.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Anderson, R. et al., 2013. Measuring the Changing Cost of Cybercrime. *The Economics of Information Security and Privacy*, pp. 265-300.

Anon., 2019. *Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_el

Anon., 2019. *Administrative fine of €170, 000 imposed on Bergen Municipality.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/administrative-fine-eu170000-imposed-bergen-municipality_el

Anon., 2019. *Administrative fines imposed on a telephone service provider.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/administrative-fines-imposed-telephone-service-provider_el

Anon., 2019. *Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_el

Anon., 2019. *BfDI imposes Fines on Telecommunications Service Providers.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_el

Anon., 2019. *Company fined 150,000 euros for infringements of the GDPR.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_el

Anon., 2019. *Danish DPA set to fine furniture company.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/danish-dpa-set-fine-furniture-company_el

Anon., 2019. *First fine by the Romanian Supervisory Authority.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_el

Anon., 2019. *ICO statement: Intention to fine British Airways £183.39m under GDPR for data breach.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-british-airways-ps18339m-under-gdpr-data-breach_el

Anon., 2019. *Polish DPA imposes €645,000 fine for insufficient organisational and technical safeguards.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_el

Anon., 2019. *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_el

Anon., 2019. *The Norwegian Data Protection Authority imposes a fine on the Municipality of Oslo, the Education Agency.* [Online] Available at: https://edpb.europa.eu/news/national-news/2019/norwegian-data-protection-authority-imposes-fine-municipality-oslo-education_en

Biener, C., Eling, M. & Wirfs, J. H., 2015. Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice* , pp. 131-158.

Bodin, L. D., Gordon, L. A., Loeb, M. P. & Wang, A., 2018. Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, Δεκέμβριος, pp. 527-544.

Bohme, R. & Kataria, G., 2006. *Models and Measures for Correlation in Cyber-Insurance.* [Online] Available at: https://core.ac.uk/download/pdf/162458449.pdf

Böhme, R. & Kataria, G., 2006. Models and Measures for Correlation in Cyber-Insurance. *Workshop on the Economics of Information Security (WEIS)*, Ιούνιος, pp. 1-26.

Brockett, P. L., Golden, L. L. & Wolman, W., 2012. Enterprise Cyber Risk Management. In: J. Emblemsvag, ed. *Risk Management for the Future: Theory and Cases.* s.l.:InTech, pp. 319-320.

Caldwell, T., 2015. Securing small businesses – the weakest link in a supply chain?. *Computer & Fraud Security*, Σεπτέβριος, pp. 5-10.

Campbell, K., Gordon, L., Loeb, M. & Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, pp. 431-448.

Cavusoglu , H., Mishra, B. & Raghunathan, S., 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, Δεκέμβριος, pp. 70-104.

Cebula , J. J. & Young, L. R., 2010. A Taxonomy of Operational Cyber Security Risks. *Carnegie Mellon University*, Δεκέμβριος, pp. 1-48.

Christoph Ritzer & Natalia Filkina, 2019. *First multi-million GDPR fine in Germany: €14.5 million for not having a proper data retention schedule in place.* [Online] Available at: https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/

Datoo, A., 2018. Data in the post-GDPR world. *Computer Fraud & Security*, Σεπτέμβριος, pp. 17-18.

De Hert, P. & Papakonstantinou , V., 2016. The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*, p. 179–194.

Eling, M. & Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*, Νοέμβριος, pp. 474-491.

Ernest & Young, 2018. *How can you disrupt risk in an era of digital trasformation?.* [Online] Available at: https://www.ey.com/Publication/vwLUAssets/ey-how-can-you-disrupt-risk-in-an-era-of-digital-transformation/$FILE/ey-how-can-you-disrupt-risk-in-an-era-of-digital-transformation.pdf

Fielder, A. et al., 2016. Decision support approaches for cyber security investment. *Decision Support Systems*, Ιούνιος, pp. 13-23.

Galligan, M. E., Herrygers, S. & Rau, K., 2019. *Managing Cyber Risk in a digital age.* [Online] Available at: https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Garber, J. & Focus, M., 2018. GDPR – compliance nightmare or business opportunity?. *Computer Fraud & Security*, Ιούνιος, pp. 14-15.

Gordon, . L. A., Loeb, M. P. & Sohail, T., 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM*, Μάρτιος, pp. 81-85.

Goucher, W., 2011. Do SMEs have the right attitude to security?. *Computer Fraud & Security*, Ιούλιος, pp. 18-20.

Hall, M., 2016. Why people are key to cyber-security. *Network Security* , Ιούνιος, pp. 9-10.

Hovav, A. & D'Arcy, J., 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, pp. 97-121.

ICAP, 2019. *ICAP GDPR SURVEY.* [Online] Available at: https://dir.icap.gr/mailimages/GDPR_NEWSurvey.pdf

James, L., 2018. Making cyber-security a strategic business priority. *Network Security*, Μάιος, pp. 6-8.

Jay, J., 2019. *teiss.co.uk.* [Online]
Available at: https://www.teiss.co.uk/danish-dpa-fines-iddesign/

Kelion, L., 2019. *Internet provider faces big GDPR fine for lax call centre checks.* [Online]
Available at: https://www.bbc.com/news/technology-50744333

Krog, G., 2019. *Norwegian DPA to fine Bergen municipality for infringement of GDPR data security requirements.* [Online] Available at: https://blog.signatu.com/blog/2019/01/08/norwegian-dpa-to-fine-city-of-bergen-for-gdpr-breach/

Krystlik, J., 2017. With GDPR, preparation is everything. *Computer Fraud & Security*, Ιούνιος, pp. 5-8.

Kurpjuhn, T., 2015. The SME security challenge. *Computer Fraud & Security*, Μάρτιος, pp. 5-7.

Livanis E., & Karagianni K., 2017. *Survey: Cyber Risk & Accounting Firms in Cyprus, International Accounting Bulletin*. [Online] Available at: http://www.internationalaccountingbulletin.com/comments/survey-cyber-risk-accounting-firms-in-cyprus-5860847

Lunden, I., 2019. *UK's ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users.* [Online] Available at: https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAADlGM8XHWPXJ2W9OhlmbA9XWT0aKIWDm96YWJV1WKj

Maillart, T. & Sornette, D., 2010. Heavy-tailed distribution of cyber-risks. *The European Physical Journal B volume*, Απρίλιος, p. 357–364.

Marotta, A. et al., 2017. Cyber-Insurance Survey. *Computer and Science Review*, Μάιος, pp. 35-61.

McCall, B., 2018. What does the GDPR mean for the medical community?. *Lancet*, Μάρτιος, pp. 1249-1250.

McKenna, B., 2018. Measuring cyber-risk. *Network Security*, Οκτώβριος, pp. 12-14.

Miglicco, G., 2018. GDPR is here and it is time to get serious. *Computer Fraud & Security*, Σεπτέμβριος, pp. 9-12.

Muciak, K., 2019. *EUR 660k fine for GDPR breach in Poland. What can we learn about the Polish DPA from the Morele.net decision?.* [Online] Available at: https://www.linkedin.com/pulse/eur-660k-fine-gdpr-breach-poland-what-can-we-learn-polish-muciak

Mukhopadhyay, A. et al., 2005. Insurance for Cyber-risk: A Utility Model. *Decision*, pp. 154-169.

Narendra, M., 2019. *PwC fined €150,000 by Hellenic Data Protection Authority.* [Online] Available at: https://gdpr.report/news/2019/07/31/pwc-fined-e150000-by-greek-data-protection-authority/

National Association of Insurance Commissioners (NAIC), 2013. *Cyber Risk.* [Online] Available at: https://content.naic.org/cipr_topics/topic_cybersecurity.htm

Öğüt, H., Raghunathan, S. & Menon, N., 2011. Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, Μάρτιος, pp. 497-512.

Panic, S., 2019. *Austria: Data Protection Authority imposes EUR 18 million fine on Austrian Post.* [Online] Available at: https://www.lexology.com/library/detail.aspx?g=7865633f-6ad1-4919-911f-81c11ec65567

Pate-Cornell, M.-E., Kuypers, M., Smith, M. & Keller, P., 2018. Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, pp. 226-241.

Paul, S., 2017. Reinforcing your SME against cyberthreats. *Computer Fraud & Security*, Οκτώβριος, pp. 13-15.

Politou, E. et al., 2018. Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, Δεκέμβριος, pp. 1247-1257.

Poritskiy, N., Oliveira, F. & Almeida, F., 2019. The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, pp. 510-524.

Power, R., 2002. CSI/FBI computer crime and security survey.. *Computer Security Issues and Trends*, Ιανουάριος, pp. 1-22.

Ryz, L., Grest, L. & Ontrack, K., 2016. A new era in data protection. *Computer Fraud & Security*, Μάρτιος, pp. 18-20.

Satariano, A., 2019. *Google Is Fined $57 Million Under Europe's Data Privacy Law*. [Online] Available at: https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Sinanaj, G. & Muntermann, J., 2013. Assessing corporate reputational damage of data breaches: an empirical analysis. *Proceedings of the 26th International Bled eConference*, pp. 78-89.

Stanciu, V. & Rîndașu, S.-M., 2018. The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania. *Journal of Information Assurance & Cyber security* , Δεκέμβριος, pp. 1-9.

Takahashi, D., 2018. *IBM security study: Mega data breaches cost $40 million to $350 million.* [Online] Available at: https://venturebeat.com/2018/07/10/ibm-security-study-mega-data-breaches-cost-40-million-to-350-million/

Teixeira, G. A., Da Silva, M. M. & Pereira, R., 2019. The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, pp. 402-418.

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*, Φεβρουάριος, pp. 134-153.

Vlachou, Z.-P., 2019. *Hellenic DPA fines for violations of data protection by design and default.* [Online] Available at: https://www.datenschutz-notizen.de/hellenic-dpa-fines-for-violations-of-data-protection-by-design-and-default-4723680/

Zerlang, J., 2017. GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, Ιούνιος, pp. 8-11.

Ομάδας Εργασίας του ΣΕΒ, 2018. *Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης.* [Online] Available at: https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

ΠΑΡΑΡΤΗΜΑ

ΜΟΡΦΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

E1
Είστε ενημερωμένοι για το νέο Ευρωπαϊκό Κανονισμό (5419/16), που αφορά την προστασία προσωπικών δεδομένων και τέθηκε σε εφαρμογή στις 25 Μαΐου 2018;
(1) Ναι (2) Όχι

E2
Κατά πόσο έχει επηρεαστεί το επάγγελμα του λογιστή μετά από τις αλλαγές που έχει επιφέρει η υποχρεωτική εφαρμογή του νέου Ευρωπαϊκού Κανονισμού (5419/16), που αφορά την προστασία προσωπικών δεδομένων;
(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

E3
Έχετε λάβει μέτρα προκειμένου να συμμορφωθείτε με τις διατάξεις του νέου Ευρωπαϊκού Κανονισμού (5419/16), που αφορά την προστασία προσωπικών δεδομένων;
(1) Ναι (2) Όχι

E4
Επιλέξτε ποιο/ποια από τα παρακάτω μέτρα εφαρμόζετε για να προστατεύσετε τα προσωπικά δεδομένα που διαχειρίζεστε ως λογιστικό γραφείο;
(1) Ενημέρωση - εκπαίδευση του προσωπικού για ευαισθητοποίηση σε θέματα ασφαλείας
(2) Εγκατάσταση και χρήση ενημερωμένων προγραμμάτων antivirus, firewalls κλπ
(3) Αλλαγή κωδικών πρόσβασης ανά τακτά χρονικά διαστήματα
(4) Back up της βάσης δεδομένων ανά τακτά χρονικά διαστήματα
(5) Τεχνολογικά μέτρα π.χ. κρυπτογράφηση
(6) Ύπαρξη πολιτικής για την ασφάλεια και αντιμετώπιση των περιστατικών απώλειας προσωπικών δεδομένων
(7) Κανένα από τα παραπάνω

E5
Έχετε έγγραφη συγκατάθεση των πελατών σας που σας επιτρέπει να διαχειρίζεστε τα προσωπικά τους δεδομένα;
(1) Ναι (2) Όχι

Ε6
Επιλέξτε ποιο/ποια από τα παρακάτω δικαιώματα έχουν οι πελάτες σας από τη στιγμή που διατηρείτε προσωπικά τους δεδομένα;

(1) Δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα
(2) Δικαίωμα ενημέρωσης/διόρθωσης/διαγραφής των προσωπικών τους δεδομένων
(3) Δικαίωμα ανάκλησης της συγκατάθεσης τους για διαχείριση των προσωπικών τους δεδομένων
(4) Κανένα από τα παραπάνω

Ε7α
Κάνετε χρήση υπηρεσιών cloud (π.χ. Google Drive, Dropbox, WeTransfer κλπ) στο λογιστικό σας γραφείο;

(1) Ναι (2) Όχι

Ε7β
Αν απαντήσατε **ΝΑΙ** στην προηγούμενη ερώτηση, πιστεύετε ότι η χρήση των υπηρεσιών αυτών σας καθιστούν περισσότερο ευάλωτους απέναντι σε κινδύνους απώλειας ή διαρροής των προσωπικών δεδομένων που διαχειρίζεστε ως λογιστικό γραφείο;
(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ε8
Σε ποιο βαθμό πιστεύετε ότι ένα περιστατικό παραβίασης της ασφάλειας των προσωπικών δεδομένων θα έχει επιπτώσεις (π.χ. οικονομικές, φήμης κλπ) για το λογιστικό σας γραφείο;
(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ε9α
Έχετε ενημερωθεί σχετικά με την ύπαρξη ασφαλιστήριων συμβολαίων κάλυψης από ηλεκτρονικούς και διαδικτυακούς κινδύνους (cyber insurance) ;

(1) Ναι (2) Όχι

Ε9β
Αν απαντήσατε **ΝΑΙ** στην προηγούμενη ερώτηση, κατά πόσο είστε διατεθειμένοι να προβείτε στην αγορά ενός τέτοιου ασφαλιστήριου συμβολαίου προκειμένου να καλύψετε τις χρηματοοικονομικές σας επιπτώσεις;
(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

Ε10
Θεωρείτε ότι η εφαρμογή του νέου Ευρωπαϊκού Κανονισμού (5419/16) έχει ευεργετικά αποτελέσματα για την προστασία των προσωπικών δεδομένων που διαχειρίζεται το γραφείο σας;
(1) Καθόλου (2) Λίγο (3) Μέτρια (4) Πολύ (5) Πάρα πολύ

<u>Δημογραφικά στοιχεία</u>

Δ1 Φύλο
1. □ Άντρας
2. □ Γυναίκα

Δ2 Ηλικία
1. □ 18-25 ετών

2. □ 26-35 ετών
3. □ 36-45 ετών
4. □ 46-55 ετών
5. □ 56-65 ετών
6. □ Άνω των 66 ετών

Δ3 Ιδιότητα στην επιχείρηση

1. □ Ιδιοκτήτης
2. □ Υπάλληλος

Δ4 Έτη λειτουργίας επιχείρησης

1. □ Λιγότερο από 1 έτος
2. □ 1-4 έτη
3. □ 5-9 έτη
4. □ 10-20 έτη
5. □ 21-31 έτη
6. □ Περισσότερα από 31 έτη