ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΛΟΓΙΣΤΙΚΗ ΦΟΡΟΛΟΓΙΑ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

Διπλωματική Εργασία

"*Οι χρημοτοοικονομικές επιπτώσεις των κινδύνων του κυβερνοχώρου στο κλάδο της εστίασης*"

Του

Μπαπαλιάρη Θανάση

Α.Μ: mas17018

Επιβλέπων Καθηγητής: Λιβάνης Ευστράτιος

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη
ΠΜΣ Λογιστική Φορολογία και Χρηματοοικονομική Διοίκηση
(ΠΜΣ Στρατηγική Διοικητική Λογιστική και τη Χρηματοοικονομική Διοίκηση)

Δεκέμβρης 2019

Ευχαριστίες

Πριν την παρουσίαση των αποτελεσμάτων της παρούσας διπλωματικής εργασίας, αισθάνομαι την υποχρέωση να ευχαριστήσω θα ήθελα να ευχαριστήσω τον καθηγητή μου Λιβάνη Ευστράτιο για την πολύτιμη καθοδήγηση του. Επίσης, θέλω να ευχαριστήσω τους γονείς μου που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου εργασίας.

Περίληψη

Στην προτεινόμενη εργασία θα μελετηθούν οι χρηματοοικονομικές επιπτώσεις των κινδύνων του Κυβερνοχώρου στο χώρο της εστίασης. Σε μια εποχή που βασικό της χαρακτηριστικό είναι η τεχνολογική και η οικονομική ανάπτυξη, στην οποία το διαδίκτυο πρωτοστατεί αποτελώντας σημαντικό εργαλείο των επιχειρήσεων, λειτουργώντας ως σημαντικός μοχλός επικοινωνίας με τους καταναλωτές, οι πιθανοί κίνδυνοι είναι πολλοί και μπορεί να έχουν σημαντικές επιπτώσεις, για τις επιχειρήσεις. Η παρούσα λοιπόν εργασία αποσκοπεί στη μελέτη του θεμελιώδους δικαιώματος στην ιδιωτικότητα των προσωπικών δεδομένων, παραθέτοντας το Γενικό Κανονισμό Προστασίας Δεδομένων γνωστός και ως GDPR 2016/679 (General Data Protection Regulation 2016/679). Ακολούθως, στο παρόν κείμενο παρουσιάζονται οι Κίνδυνοι του Κυβερνοχώρου (Cyber Risks), αποσκοπώντας τελικά στην ανάδειξη των χρηματοοικονομικών επιπτώσεων αυτών στο χώρο της εστίασης.

Abstract

This paper will examine the financial implications of the cyber risks in the catering industry. At a time when technology and economic development are at the forefront, where the Internet is at the forefront of being an important business tool, acting as an important lever for consumers, the potential risks are many and can have a significant impact on businesses. The present paper therefore aims to study the fundamental right to privacy of personal data, citing the General Data Protection Regulation also known as GDPR 2016/679 (General Data Protection Regulation 2016/679). In the following, the Cyber Risks are presented in this text, ultimately aiming to highlight these financial impacts on the catering industry.

Περιεχόμενα

Κεφάλαιο πρώτο

1.1 Εισαγωγή

Ο σεβασμός στην ιδιωτική ζωή, συνιστά θεμελιώδες δικαίωμα του ανθρώπου και η προστασία του κατοχυρώθηκε ήδη από τα συνταγματικά κείμενα του 18ου αιώνα. Στα σύγχρονα κείμενα, το δικαίωμα στην ιδιωτική ζωή αναγνωρίζεται το έτος 1948, μέσω της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου. Ειδικότερα, η διακήρυξη αναφέρει χαρακτηριστικά, όπως περιγράφουν οι Κοτσάλης και Μενοδάκης (2018), *«ο καθένας έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, του σπιτιού και της αλληλογραφίας του»*. Έτσι εύκολα, μπορεί να συμπεράνει κανείς ότι η Ευρωπαϊκή Ένωση προσπάθησε να εξασφαλίσει την προστασία του δικαιώματος αυτού μέσω της νομοθεσίας.

Με το πέρασμα των χρόνων και ενώσω η τεχνολογία λάμβανε μεγάλο μέρος της καθημερινής ζωής, η Ευρωπαϊκή Επιτροπή αναγνώρισε την ανάγκη να ληφθούν νέες προφυλάξεις εναρμονισμένες με τις σύγχρονες ανάγκες. Έτσι, το 1995 ενέκρινε την ευρωπαϊκή οδηγία για την προστασία των δεδομένων, θεσπίζοντας ελάχιστα πρότυπα για την ιδιωτική ζωή και την ασφάλεια, βάσει των οποίων κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης βασίζεται στον δικό του νόμο εφαρμογής. Με το τρόπο αυτό, θεμελιώθηκε η έννοια της προστασίας των προσωπικών δεδομένων, ως αυτοτελές δικαίωμα. Θα μπορούσε μάλιστα να ειπωθεί ότι το δικαίωμα αυτό αποτελεί μια εξειδίκευση των Δικαιωμάτων του Ανθρώπου, όπως αυτά διατυπώθηκαν το 1948, δεδομένου ότι επικεντρώνονται στη προστασία των προσωπικών δεδομένων σε μια προσπάθεια διαφύλαξης της ελευθερίας και των δικαιωμάτων του ανθρώπου έναντι στην ιδιωτικότητα του. Σημαντικό είναι να αναφερθεί ότι όσον αφορά τη προστασία των δεδομένων, οι Κοτσαλής και Μενουδάκης (2018), αναφέρουν ότι το 1981, καταρτίστηκε η Διεθνής Σύμβαση 108, που σκοπό είχε τη προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία όμως τέθηκε σε ισχύ τη 1η Οκτώβρη ου 1985.

Μερικά χρόνια αργότερα, το 1995, προστασία των προσωπικών δεδομένων, επικαιροποιήθηκε νομικά μέσω της Οδηγίας 95/46/ΕΚ για την προστασία των

προσωπικών δεδομένων, η οποία μεταφέρθηκε στο εθνικό δίκαιο με το Ν. 2472/19972. Ο νόμος αυτός, αποτέλεσε την αφορμή για την συνταγματική κατοχύρωση της προστασίας των προσωπικών δεδομένων, αφού κατά τη συνταγματική αναθεώρηση του 2001, προστέθηκε το άρθρο 9Α του Συντάγματος το οποίο, αναγνωρίζει το δικαίωμα προστασίας των προσωπικών δεδομένων, το οποίο και διασφαλίζει μέσω της θέσπισης ανεξάρτητης αρχής (Καρατζά, 2014). Το σημαντικό αυτό νομικό βήμα, με τη προσθήκη της Οδηγίας 95/46/ΕΚ διασφαλίζεται η προστασία των προσωπικών δεδομένων, ανάγοντας της πλέον σε ένα αυτοτελές ατομικό δικαίωμα που χρήζει προστασίας από ένα ολοκληρωμένο και οριοθετημένο νομικό πλαίσιο, δηλαδή παύει να αντιμετωπίζεται ως μια έκφανση της ιδιωτικότητας αλλά λαμβάνει νομικό και συνταγματικό χαρακτήρα. Έτσι, παρά το γεγονός ότι η 95/46/ΕΚ βοήθησε στην εναρμόνιση των εθνικών νομοθεσιών των κρατών μελών, αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, η φύση της ως Οδηγίας, οι τεχνολογικές εξελίξεις που επηρέασαν τη λειτουργία των επιχειρήσεων, η παγκοσμιοποίηση, που έθεσε νέα θεμέλια στον επιχειρηματικό κόσμο και κυρίως η ραγδαία ανάπτυξη του διαδικτύου και η σύγκληση των οικονομικών δραστηριοτήτων, δημιούργησαν νέα ζητήματα, πιο εξειδικευμένα που απαιτούσαν διεξοδικότερη ανάλυση και προσοχή. Κρίνεται σημαντικό να τονισθεί, ότι η Οδηγία 95/46/ΕΚ, υιοθετήθηκε σε μια εποχή όπου η χρήση του διαδικτύου και των τεχνολογικών μέσων ήταν σε πρώιμα στάδια, όπου η χρήση κα η εφαρμογή τους δεν είχαν σημαντικό αντίκτυπο στη καθημερινή ζωή μεταξύ των συναλλασσομένων. Εύκολα λοιπόν γίνεται αντιληπτό, ότι στη νέα αυτή πραγματικότητα, η ανάπτυξη ενός νέου νομοθετήματος για τη προστασία των προσωπικών δεδομένων, υπό ένα πλέγμα προστασίας ισχυρότερο από αυτό που είχε θεσπιστεί το 1995 είναι επιτακτικής ανάγκης (Μήτρου, 2017).

Κρίσιμο στοιχείο, συνεπώς, αποτελεί η τεχνολογική εξέλιξη και συνακόλουθα, ο αντίκτυπός της στην διαχείριση των προσωπικών δεδομένων. Πλέον η ροή των πληροφοριών και των δεδομένων δεν περιορίζεται στα στεγανά όρια των γεωγραφικών αποστάσεων. Ένα χαρακτηριστικό της σύγχρονης εποχής που αξιοποιήθηκε από τις εταιρείες και τις επιχειρήσεις για την ενίσχυση της παραγωγικότητας και της οικονομικής τους ανάπτυξης, μέσω της συλλογής δεδομένων που αφορούσαν στις προτιμήσεις ενός προσώπου ως καταναλωτή, προκειμένου να συγκεντρώσουν στοιχεία για τις προτιμήσεις ενός προσώπου ως

καταναλωτή και να διαμορφώσουν στοχευμένα τόσο την διαφημιστική τους πολιτική, όσο και την προώθηση των προϊόντων τους. Παρατηρείται πλέον ότι οι προσωπικές πληροφορίες, συνιστούν οικονομικό μέγεθος όχι μόνο για τις επιχειρήσεις, αλλά και για τον κρατικό μηχανισμό (Μήτρου, 2017). Υπό το πρίσμα αυτό, στις αρχές της δεκαετίας του 2010 εντάθηκε ο προβληματισμός, αναφορικά με την αναγκαιότητα αναθεώρησης της Οδηγίας 95/46/ΕΚ ή ακόμη και αντικατάστασής της από ένα νέο αποτελεσματικότερο κανονιστικό πλαίσιο.

Κάποια χρόνια αργότερα, τον Ιανουάριο του 2012, σύμφωνα με τον Ιγγλεζάκη (2018), η Ευρωπαϊκή Επιτροπή, έπειτα από έντονες διαβουλεύσεις και συζητήσεις, κατέθεσε ένα σύνολο προτάσεων που σκοπό είχαν τη ριζική αναθεώρηση του ρυθμιστικού πλαισίου κανόνων για την προστασία των φυσικών προσώπων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με απώτερο σκοπό να αποκατασταθεί η εμπιστοσύνη στην ευρωπαϊκή νομοθεσία αναφορικά με τα προσωπικά δεδομένα και τους όρους προστασίας και επεξεργασίας τους. Τελικά, τον Απρίλιο του 2016, υπεγράφη ο Κανονισμός 2016/679 (Regulation 2016/679) ή Γενικός Κανονισμός για τη Προστασία Δεδομένων, γνωστός και ως GDPR 2016/679 (General Data Protection Regulation 2016/679), που σκοπό είχε να ισχυροποιήσει νομοθετικά τη προστασία των προσωπικών δεδομένων.

Βέβαια, στις μέρες μας είναι ευρέως διαδεδομένο πλέον ότι κάθε επιχείρηση με έδρα της την Ευρωπαϊκή Ένωση, όπως και κάθε άλλη επιχείρηση εγκατεστημένη εκτός αυτής, που όμως διαχειρίζεται προσωπικά δεδομένα πολιτών της Ευρωπαϊκής Ένωσης, είναι υποχρεωμένη να συμμορφωθεί πλήρως στις επιταγές του Γενικού Κανονισμού Προστασίας Δεδομένων ή όπως είναι γνωστό στο ευρύ κοινό στο GDPR (General Data Protection Regulation). Η ανάγκη αυτή είναι απόρροια του τρόπου λειτουργίας και παροχής υπηρεσιών από τις σύγχρονες επιχειρήσεις, όπου οι δομές και το επιχειρηματικό τους μοντέλο βασίζεται στα νέα τεχνολογικά μέσα και τους γρήγορα αναπτυσσόμενους ρυθμούς της τεχνολογίας. Συνεπώς, γίνεται εύκολα αντιληπτό πως στη νέα αυτή τάξη πραγμάτων όπου το διαδίκτυο πρωτοστατεί στις παρεχόμενες υπηρεσίες δημιουργώντας την ανάγκη κοινοποίησης προσωπικών δεδομένων των καταναλωτών στις επιχειρήσεις, ένας Γενικός Κανονισμός Προστασίας Δεδομένων κρίνεται αναγκαίος. Σημαντικό είναι να τονισθεί πως στο έντονα αυτό μεταβαλλόμενο επιχειρηματικό σκηνικό, οι επιχειρήσεις που θα καταφέρουν να μετατρέψουν τη προστασία προσωπικών δεδομένων σε πυρήνα της

καθημερινής τους λειτουργίας θα αποκτήσουν σημαντικό ανταγωνιστικό πλεονέκτημα. Άξιο λόγου βέβαια είναι ότι ένα τέτοιο εγχείρημα καθίσταται ιδιαίτερα δύσκολο και επισφαλές, δεδομένου της αστάθειας και της εύκολης πρόσβασης ή παραβίασης των νέων τεχνολογικών μέσων και του διαδικτύου. Οι κίνδυνοι του Κυβερνοχώρου, είναι πλέον ένας νέος όρος, που σκοπό έχει να περιγράψει τις δυσκολίες και τους φόβους παραβίασης των δεδομένων μέσω διαδικτύου. Είναι σαφές πως τα οφέλη της χρήσης του διαδικτύου είναι σημαντικά, ωστόσο αυτά έρχονται με έναν εγγενή κίνδυνο και ένα σύνολο τρωτών σημείων που απαιτούν μεγάλη οργάνωση και διαχείριση. Οποιαδήποτε εταιρεία σε όποιο κλάδο και αν δραστηριοποιείται έρχεται αντιμέτωπη με ζητήματα που αφορούν στη προστασία των προσωπικών δεδομένων από κινδύνους του Κυβερνοχώρου.

Η παρούσα εργασία κρίνει πολύ σημαντική την ανάληψη μέτρων διαφύλαξης από Κινδύνους παραβίασης δεδομένων και ιδιαίτερα κινδύνους του Κυβερνοχώρου, καθώς μπορεί να αποτελέσουν σημαντική ζημία για τις επιχειρήσεις με σημαντικές χρηματοκοινονομικές επιπτώσεις που είναι δύσκολο να προσπελαστούν.

1.2 Σκοπός εργασίας

Βασικός σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη των χρηματοοικονομικών επιπτώσεων των κινδύνων του κυβερνοχώρου στο κλάδο της εστίασης. Για την επίτευξη του σκοπού αυτού κρίνεται αναγκαία η μελέτη του Γενικού Κανονισμού Προστασία Δεδομένων (GDPR, General Data Protection Regulation), με σκοπό να διερευνηθεί το νομικό πλαίσιο που αφορά στη προστασία δεδομένων προσωπικού χαρακτήρα. Ακολούθως, κρίνεται σημαντικό να μελετηθούν, οι Κίνδυνοι του Κυβερνοχώρου (Cyber Risks), ειδικότητα να οριοθετηθεί σαν έννοια, ακολούθως να μελετηθούν οι πιθανοί κίνδυνοι με τους οποίους μπορεί να έρθει αντιμέτωπη μια επιχείρηση. Οι ενότητες αυτές θα μας επιτρέψουν να εξάγουμε συμπεράσματα για τις χρηματοοικονομικές επιπτώσεις των Κινδύνων του Κυβερνοχώρου στις επιχειρήσεις δίνοντας έμφαση σε εταιρείες και οργανισμούς που δραστηριοποιούνται στο χώρο της εστίασης.

1.3 Μεθοδολογική προσέγγιση για την κάλυψη των θεωρητικών στόχων: Η μέθοδος της βιβλιογραφικής ανασκόπησης

Για την κάλυψη των θεωρητικών στόχων της εργασίας χρησιμοποιείται η μέθοδος της αφηγηματικής βιβλιογραφικής ανασκόπησης (narrative bibliographic research). Αυτή η μέθοδος χρησιμοποιείται για τη συλλογή του απαραίτητου ερευνητικού υλικού με σκοπό την θεωρητική διερεύνηση του θέματος, τη διατύπωση των θεωρητικών στόχων και των ερευνητικών ερωτημάτων. Επίσης, η βιβλιογραφική ανασκόπηση συμβάλλει στη τεκμηρίωση του θέματος και στη θεωρητική διασαφήνιση των βασικών θεωρητικών εννοιών μιας εργασίας. Τέλος η βιβλιογραφική ανασκόπηση δίνει τη δυνατότητα στο μελετητή να αποφύγει άκαρπες ερευνητικές προσεγγίσεις εντοπίζοντας και αξιολογώντας κριτικά τα ευρήματα άλλων μελετών (Πατελάρου & Μπροκαλάκη, 2010, σελ. 121).

Βασικό υλικό της βιβλιογραφικής ανασκόπησης αποτελούν διεθνείς μελέτες, ακαδημαϊκά άρθρα, επιστημονικά βιβλία και πηγές από το διαδίκτυο που ασχολούνται με το υπό εξέταση θέμα.

Για την απάντηση των ερευνητικών ερωτημάτων χρησιμοποιείται η ποσοτική μεθοδολογία έρευνας, μέσω της μελέτης περιπτώσεων που θα αντιστοιχούν σε επιλεγμένα, μη διασυνδεδεμένες επιχειρήσεις του Ελλαδικού χώρου με διαφορετικά χαρακτηριστικά. Η ποσοτική έρευνα δίνει τη δυνατότητα στον ερευνητή να μελετήσει σε βάθος ένα φαινόμενο διερευνώντας τα χαρακτηριστικά, τις εφαρμογές και τους περιορισμούς ή/και τις δυνατότητες των επιχειρήσεων. Τέλος, να σημειωθεί ότι η βιβλιογραφική έρευνα στα σημαντικότερα σημεία της παρούσας εργασίας σε συνδυασμό με τη ποσοτική έρευνα που πραγματοποιείται σε είκοσι επιχειρήσεις στον Ελλαδικό χώρο, καθιστούν τη μελέτη.

Οι θεωρητικοί και ερευνητικοί στόχοι της εργασίας παρουσιάζονται στο πίνακα που ακολουθεί:

Πίνακας 1.1: θεωρητικοί και ερευνητικοί στόχοι

Θεωρητικοί στόχοι	**Ερευνητικοί στόχοι**
Ανάδειξη του Γενικού Κανονισμού Προστασίας Δεδομένων.	
Εννοιολογική αποσαφήνιση των Κινδύνων του Κυβερνοχώρου.	
Προσδιορισμών των επιπτώσεων και ειδικότερα των χρηματοοικονομικών επιπτώσεων των Κινδύνων του Κυβερνοχώρου στο χώρο της εστίασης.	

Τα βασικά ερευνητικά ερωτήματα είναι τρία και παρουσιάζονται στον πίνακα 2.

Πίνακας 1.2: Ερευνητικά ερωτήματα

Ερευνητικό ερώτημα 1	Ποιες είναι οι επιπτώσεις των κινδύνων του κυβερνοχώρου στο κλάδο της εστίασης;
Ερευνητικό ερώτημα 2	Ποιες είναι οι στάσεις των επιχειρηματιών του κλάδου της εστίασης απέναντι στην προστασία των προσωπικών δεδομένων;

1.4 Δομή εργασίας

Για τη καλύτερη κατανόηση του παρόντος θέματος η εργασία έχει χωρισθεί σε δυο μέρη, το ***Γενικό Μέρος*** και το ***Ειδικό Μέρος,*** όπου στην πρώτη περίπτωση έχουμε την ανάπτυξη του θεωρητικού πλαισίου της εργασίας με την ανάπτυξη των αντίστοιχων κεφαλαίων που θα αναφερθούν παρακάτω και αποσκοπούν στην καλύτερη κατανόηση αλλά και ανάδειξη της σημαντικότητας του θέματος που έχει επιλεγεί.

Ειδικότερα, το Γενικό Μέρος, περιλαμβάνει το ***πρώτο κεφάλαιο,*** όπου διατυπώνεται ο προβληματισμός που ακολουθεί τη παρούσα εργασία και γίνεται μια προσπάθεια αποτύπωσης του σκοπού αλλά και των βασικών ερωτημάτων της εργασίας αυτής. Στο τέλος, του κεφαλαίου αυτού γίνεται η παρουσίαση της δομής της εργασίας για να αποδώσει τα κύρια σημεία και να βοηθήσει στη καλύτερη μελέτη του περιεχομένου του κειμένου αυτού.

Ακολούθως, το ***δεύτερο κεφάλαιο,*** περιλαμβάνει το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR, General Data Protection Regulation), ειδικότερα επιχειρεί να οριοθετήσει χρονικά την κατοχύρωση του Κανονισμού και να αναλυθεί η νομική βάση, περί προστασίας των προσωπικών δεδομένων. Το ***τρίτο κεφάλαιο***, του παρόντος κειμένου, διερευνά τους Κινδύνους του Κυβερνοχώρου (Cyber Risks), ειδικότερα γίνεται προσπάθεια της εννοιολογικής του βάσης και της ανάδειξης των πιθανών επιπτώσεων του. Το ***τέταρτο κεφάλαιο***, της παρούσας εργασίας αναφέρεται στις χρηματοοικονομικές επιπτώσεις των Κινδύνων του Κυβερνοχώρου σε επιχειρήσεις που δραστηριοποιούνται στο χώρο της εστίασης.

Εν συνεχεία, ακολουθεί το Ειδικό μέρος, όπου περιλαμβάνει το ερευνητικό μέρος της παρούσας εργασίας, ειδικότερα ***το πέμπτο κεφάλαιο*** αναφέρεται στη μεθοδολογία που αναπτύχθηκε για τη ποσοτική ανάλυση σε είκοσι επιχειρήσεις στο χώρο της εστίασης. Το ***έκτο κεφάλαιο,*** επικεντρώνεται στα αποτελέσματα της έρευνας και τέλος, η εργασία ολοκληρώνεται με τα βασικά συμπεράσματα της παρούσας εργασίας και των προτάσεων για μελλοντική έρευνα.

Κεφάλαιο δεύτερο

Γενικός Κανονισμός Προστασίας Δεδομένων

2.1 Εισαγωγή

Στις 27 Απριλίου 2016, υπεγράφη από το πρόεδρο του Ευρωπαϊκού Συμβουλίου, Martin Schulz, στις Βρυξέλλες, ο Κανονισμός 2016/679 (Regulation 2016/679) ή Γενικός Κανονισμός για τη Προστασία Δεδομένων, γνωστός και ως GDPR 2016/679 (General Data Protection Regulation 2016/679). Κρίνεται σημαντικό να αναφερθεί ότι η επεξεργασία του προαναφερθέντος Κανονισμού ξεκίνησε το 2009 και ο σχεδιασμός του πρόσταζε να εφαρμοστεί το Μάιο του 2018. Η πρόβλεψη αυτής της διετούς μεταβατικής περιόδου κρίθηκε αναγκαία προκειμένου να παρασχεθεί η δυνατότητα να ενημερωθούν και να προετοιμαστούν για την εφαρμογή των νέων ρυθμίσεων κυρίως όσοι χειρίζονται προσωπικά δεδομένα, δηλαδή οι υπεύθυνοι επεξεργασίας και οι εκτελούντες επεξεργασίας, όπως, άλλωστε, και οι αρμόδιες εποπτικές αρχές, που για τη χώρα μας, το ρόλο αυτό έχει λάβει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο DeHert (2016), αναφέρει ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων, αφορά αλλά και επηρεάζει το τρόπο συνεργασίας όλων των Ευρωπαίων πολιτών που διαμένουν εντός και εκτός της Ευρωπαϊκής Ένωσης, ενώ αφήνει ανεπηρέαστες μόνο τις μυστικές υπηρεσίες των κρατών μελών της και τις Ευρωπαϊκές υπηρεσίες επιβολής του νόμου.

Ο Κανονισμός 2016/679 (Regulation 2016/679) δεν αποτελεί ένα νέο και πρωτοπόρο νομοθέτημα και σε καμία περίπτωση δε μπορεί να χαρακτηριστεί ως μια ριζική τομή στο καθεστώς προστασίας των προσωπικών δεδομένων. Ο λόγος είναι ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων, που υπεγράφη το 2016, αποτελεί ένα νέο ενωσιακό νομοθέτημα που επιχειρεί να αντικαταστήσει την Οδηγία 95/46/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24^{ης} Οκτωβρίου 1995, για τη προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Παράλληλα γίνεται εύκολα αντιληπτό, ότι δεν εισάγει ανατρεπτικές αντιλήψεις και επαναστατικές μεθόδους στον τρόπο αντιμετώπισης των κινδύνων για την ιδιωτικότητα. Κατά βάση επαναπροσδιορίζει την προστασία δεδομένων προσωπικού χαρακτήρα ως θεμελιώδες δικαίωμα και κατοχυρώνει τις βασικές αρχές που είναι γνωστές από το 1995, χωρίς

όμως να αποτελεί απλή επικαιροποίηση της Οδηγίας 95/46/ΕΕ. Ορισμένες από τις αρχές αυτές, που έχουν εξειδικευθεί από την νομολογία κυρίως του Δικαστηρίου της Ευρωπαϊκής Ένωσης, αναπτύσσονται περαιτέρω και διευρύνονται και, παράλληλα, θεσπίζονται νέες διαδικασίες με σκοπό τον αποτελεσματικότερο έλεγχο του σεβασμού των κανόνων προστασίας. Γενικότερα, ο Κανονισμός αποτελεί ένα μεγάλο βήμα, ίσως και ένα άλμα στην πορεία της νομικής προστασίας της ιδιωτικότητας. Από την άποψη αυτή μπορεί να θεωρηθεί ότι δημιουργεί την επόμενη, την τέταρτη γενιά κανόνων για την προστασία των προσωπικών δεδομένων.

2.1.1 Αντικείμενο και στόχοι

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, όπως έχει περιγραφεί και παραπάνω, θεσπίζει τους κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ενώ παράλληλα οριοθετεί τους κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

Από την άλλη, έχει καταστεί σαφές ότι ο βασικός στόχος του κανονισμού είναι να διασφαλίσει τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με ιδιαίτερη έμφαση στο δικαίωμα προστασίας των προσωπικών δεδομένων. Η ενδελεχή ανάγνωση του Κανονισμού 2016/679 και ειδικότερα του άρθρου 1, υποστηρίζει τα άνωθι, καθώς αναφέρει χαρακτηριστικά ότι *«ότι η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα».* Συνεπώς, Παράλληλα, στο άρθρο 2, στου ίδιου Κανονισμού προσδιορίζεται ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων, εφαρμόζεται στην, *«εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης»*.

Η παραπάνω φράση συμπληρώνεται από τις αναφορές στο τρίτο άρθρο του σχετικού κανονισμού στο οποίο αναφέρεται ότι το πεδίο εφαρμογής του εμπίπτει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ευρωπαϊκή Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ευρωπαϊκής Ένωσης. Επιπλέον, ο κανονισμός εφαρμόζεται για την

επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου. Ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ευρωπαϊκή Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

➢ Την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ευρωπαϊκή Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή

➢ Την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ευρωπαϊκής Ένωσης.

2.1.2 Αρχές που Διέπουν την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, μεταξύ άλλων έχει οριοθετήσει με σαφήνεια τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, στο άρθρο 5 του Κανονισμός 2016/679, παρατίθεται ότι τα δεδομένα προσωπικού χαρακτήρα *«υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων».* Μέσω του προαναφερθέντος νόμου, ο Κανονισμός επιχειρεί να διασφαλίσει τη νομιμότητα, την αντικειμενικότατα αλλά και τη διαφάνεια αναφορικά με την επεξεργασία δεδομένων Ευρωπαίων πολιτών, εντός και εκτός αυτής. Παράλληλα, στον ίδιο νόμο, περιγράφεται ότι τα δεδομένα προσωπικού χαρακτήρα, *«συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς*». Η παράγραφος αυτή του άρθρου 5, επιχειρεί να περιορίσει το σκοπό της συλλογής δεδομένων προσωπικού χαρακτήρα, ενώ με τη παράγραφο που ακολουθεί, επιχειρεί να οριοθετήσει την επεξεργασία αυτών, μέσω ελαχιστοποίησης των δεδομένων. Συγκεκριμένα, αναφέρεται ότι τα δεδομένα προσωπικού χαρακτήρα *«είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για*

τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία». Επιπρόσθετα, κρίνεται σημαντικό να αναφερθεί ότι ο Κανονισμός περιγράφει ρητά ότι τα δεδομένα που θα παρασχεθούν στην εκάστοτε επιχείρηση, θα πρέπει να είναι ακριβή και τότε μόνον να επικαιροποιούνται, ενώ παράλληλα τονίζει ότι πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Να αναφερθεί ότι τα δεδομένα προσωπικού χαρακτήρα, σύμφωνα πάντα με το άρθρο 5, του Κανονισμού 2016/679, πρέπει να *«διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων».* Συμπερασματικά, μέσω της παραγράφου αυτής, γίνεται προσπάθεια περιορισμού της περιόδου αποθήκευσης των δεδομένων, γεγονός που διασφαλίζει το υποκείμενο από την κακόβουλη έκθεση αυτών. Όσον αφορά βέβαια το τρόπο επεξεργασίας των δεδομένων, ο Κανονισμός εγγυάται ότι θα πραγματοποιείται με ασφάλεια, προστατεύοντας τα, από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων, διασφαλίζοντας με το τρόπο αυτό την ακεραιότητα και την εμπιστευτικότητα. Κλείνοντας, τη παράγραφο αυτή, στην οποία παρουσιάστηκαν οι αρχές που διέπουν την επεξεργασία δεδομένων, κρίνεται σημαντικό να σημειωθεί ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τα όσα προβλέπονται στο Κανονισμό, ενισχύοντας έτσι την λογοδοσία.

2.1.3 Νομιμότητα της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, έχει ορίσει και τις περιπτώσεις κατά τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα, μπορούν να θεωρηθούν νόμιμες. Οι προϋποθέσεις κατά τις οποίες μπορεί να μπορεί να θεωρηθεί νόμιμη η επεξεργασία δεδομένων των υποκειμένων περιγράφονται στο άρθρο 6 του Κανονισμού 2016/679. Ειδικότερα, αναφέρεται ότι η επεξεργασία μπορεί να χαρακτηριστεί ως σύννομη ότι *«το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς»* ή όταν «η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης». Συμπερασματικά, βάση των δύο αυτών παραγράφων, η επεξεργασία γίνεται στη περίπτωση όπου το υποκείμενο των δεδομένων είναι γνώστης και συναινεί με τη πράξη αυτή. Κατ' ουσίαν, δίνεται η δυνατότητα στο υποκείμενο να αποφασίσει για τα προσωπικά του δεδομένα. Από την άλλη, στο ίδιο άρθρο του Κανονισμού, αναφέρεται πως υπάρχει νομιμότητα όταν *«η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας ή για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου».* Τέλος, κλείνοντας, με τη παράγραφο αυτή που αφορά στην επεξεργασία των προσωπικών δεδομένων του υποκειμένου, κρίνεται σημαντικό να αναφερθεί ότι είναι αποδεκτή η επεξεργασία όταν αυτή *«είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί».* Εν κατακλείδι, γίνεται εύκολα αντιληπτό ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων, επιχειρεί να διαφυλάξει τα δικαιώματα και τις ελευθερίες των υποκειμένων και να διασφαλίσει ότι αυτοί θα έχουν κατά κύριο έλεγχο της επεξεργασίας των δεδομένων τους.

2.1.4 Διαφανής Ενημέρωση

Από τα σημαντικότερα σημεία του Γενικού Κανονισμού Προστασίας Δεδομένων, αποτελεί η διαφανής ενημέρωση και η συγκατάθεση του υποκειμένου για τη χρήση των δεδομένων του. Μιας και ο παράγοντας αυτός, δηλαδή της ενημέρωσης και συγκατάθεσης είναι υψίστης σημασίας, δε θα μπορούσε σε καμία περίπτωση να μη ληφθεί υπόψη και να μην οριοθετηθεί νομικά. Για το εν λόγο θέμα το άρθρο 7 του Κανονισμού 2016/679, αναφέρει ότι, *«όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση».*

Ο κανονισμός ωστόσο, παρέχει τη δυνατότητα στο υποκείμενο των δεδομένων να ανακαλέσει τη συγκατάθεση του, οποιαδήποτε στιγμή ο ίδιος το αποφασίσει. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της. Επιπροσθέτως, κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

Αφού παραπάνω έγινε αναφορά για τη συγκατάθεση και τη δυνατότητα του υποκειμένου να ανακαλέσει για τη χρήση των προσωπικών του δεδομένων, κρίνεται σημαντικό να αναφερθούμε στη διαφανή ενημέρωση, το οποίο περιγράφεται στο άρθρο 12, περί της διαφανούς ενημέρωσης, ανακοίνωσης και των ρυθμίσεων για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων, επεξηγείται περαιτέρω *«ότι ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των δεδομένων του, σε συνοπτική, διαφανή, κατανοητή και εύκολα*

προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά». Οι πληροφορίες που παρέχονται στο υποκείμενο δίνονται γραπτώς, ωστόσο δεν είναι περιοριστικό αυτός, μιας και μπορούν να δοθούν και με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα. Εύκολα γίνεται αντιληπτό ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δίνει μεγάλη έμφαση στη συγκατάθεση του υποκειμένου για τη χρήση των δεδομένων του, ενώ παράλληλα κρίνει σημαντική και την ορθή ενημέρωση του υποκειμένου με κάθε μέσω, μόνο που θα πρέπει να δίνεται έμφαση στη ταυτοποίηση του και με άλλα μέσα.

Όσον αφορά την ενημέρωση, κρίνεται σημαντικό να αναλυθούν οι πληροφορίες που δίνονται στο υποκείμενο των δεδομένων, τα οποία περιγράφονται στο άρθρο 13 και 14 του Κανονισμού 2016/679. Σημαντικό είναι να αναδειχθεί ότι και στους δυο νόμους που έχουν αναφερθεί, οι πληροφορίες που δίνεται στο υποκείμενο είναι κοινές. Η διαφορά έγκειται στο τρόπο συλλογής των δεδομένων αυτών, ειδικότερα, εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων, ο κανονισμός εμπίπτει στο άρθρο 13, εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεχθεί από το υποκείμενο των δεδομένων, τότε περιγράφονται από το άρθρο 14.. Βάσει των όσων αναφέρονται, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες:

- ✓ Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας.
- ✓ Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση.
- ✓ Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία.
- ✓ Τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο.

- ✓ Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν.
- ✓ Κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.

2.1.5 Δικαίωμα Διόρθωσης, Διαγραφής, Εναντίωσης και Περιορισμού της Επεξεργασίας

Τέλος, στην ενότητα αυτή, θα αναφερθούμε στο δικαίωμα του υποκειμένου να διορθώσει, να διαγράψει, να εναντιωθεί και να περιορίσει την επεξεργασία των δεδομένων του. Τα άνωθι συνοψίζονται στο άρθρο 16, όπου αναφέρεται ότι *«το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης».*

Όσον αφορά την διαγραφή των προσωπικών δεδομένων, στο άρθρο 17 αναφέρεται ότι *«το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους»:*

- ✓ Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
- ✓ Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.

- ✓ Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία.
- ✓ Τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα.
- ✓ Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.
- ✓ Τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών.

2.2 Αποτίμηση Γενικού Κανονισμού Προστασίας Δεδομένων

Στη προηγούμενη ενότητα, συζητήθηκε έντονα το περιεχόμενο του Γενικού Κανονισμού Προστασίας Δεδομένων, βέβαια στο παρόν κείμενο κρίνεται σημαντικό να μελετηθεί η σημαντικότητα και η σημασία αυτού. Στη προσπάθεια εξεύρεσης κειμένων που θα παρέχουν μια ενδελεχή επισκόπηση των συζητήσεων, καθώς και των προκαταρκτικών εγγράφων που προηγήθηκαν της δημοσίευσης του Γενικού Κανονισμού Προστασίας Δεδομένων, βρέθηκε το άρθρο των Hert και Papakonstantinou (2016), που παρέθεσαν τις θέσεις τους αναφορικά με την αποτελεσματικότητα του νέου αυτού Κανονισμού για την προστασία των προσωπικών δεδομένων, συγκρίνοντας, κατά κύριο λόγο, τα αρχικά κείμενα της Κομισιόν επί του θέματος και τις μεταγενέστερες σχετικές δημοσιεύσεις. Σύμφωνα με τους συγγραφείς, *«αν και ορισμένες αλλαγές και τροποποιήσεις στο κείμενο του Κανονισμού, εγείρουν σημαντικά ερωτήματα και συζητήσεις, εντούτοις ο αυτοσκοπός του παρέμεινε αναλλοίωτος»*, και για τον λόγο αυτό όπως αναφέρουν στο κείμενο τους επικροτούν τόσο τον ερχομό του νέου αυτού Κανονισμού, όσο και τις θετικές αλλαγές που θα επιφέρει στην παγκόσμια κοινότητα. Ωστόσο, η πάγια θέση των επιστημόνων είναι ότι *«η Κομισιόν δεν θα πρέπει να επαναπαυθεί από την όποια επιτυχία και αποδοχή γνωρίσει ο νέος αυτός Κανονισμός, αλλά οφείλει να βρίσκεται σε συνεχή επαγρύπνηση προκειμένου να επιτυγχάνει συνεχείς βελτιώσεις και να μετριάζει τις όποιες αμβλώσεις προκληθούν στην πορεία».*

Με σαφή προσανατολισμό υπέρ της υπεράσπισης του νέου Κανονισμού περί προστασία των προσωπικών δεδομένων, φαίνεται να είναι ο Zerlang (2017), όπου στο

άρθρο του επεξηγεί συνοπτικά, τις επιπτώσεις του κανονισμού στο επιχειρηματικό γίγνεσθαι. Σύμφωνα με τον συγγραφέα, το σημαντικότερο ενδεχομένως όφελος του Γενικού Κανονισμού είναι ότι άπτεται ενός μεγάλου φάσματος εννοιών και ζητημάτων που χρήζουν αντιμετώπισης. Για τον Zerlang (2017), ο κανονισμός έχει σχεδιαστεί με γνώμονα το μέλλον, καθορίζοντας την ελάχιστη βασική γραμμή ασφάλειας στην οποία θα υπόκεινται τα δεδομένα, σε αντίθεση με την ελάχιστη απαίτηση για την εξασφάλισή τους. Επίσης τονίζει ότι το επίκεντρο είναι πολύ ευρύτερο, γεγονός που ο προηγούμενος κανονισμός δε μπορούσε να καλύψει, συνεπώς η καθιέρωση ενός νέου ήταν απαραίτητη, με το τρόπο αυτό, σύμφωνα με τον συγγραφέα, υποκινούνται οι εταιρείες να εξασφαλίσουν τα συστήματά τους για να αποφευχθούν οι παραβιάσεις δεδομένων όπου είναι δυνατόν. Αυτό σημαίνει ότι σε ένα συνεχώς εξελισσόμενο ψηφιακό τοπίο, ο κανονισμός θα πρέπει να παραμείνει σχετικός με τις σύγχρονες επιχειρηματικές πρακτικές για τα επόμενα χρόνια. Επιπροσθέτως, ο συγγραφέας σχολιάζει ότι ένα βασικό αποτέλεσμα αυτής της προσέγγισης είναι η υιοθέτηση ανθεκτικών και συνεκτικών δομών στον κυβερνοχώρο (cyber- resilience), μιας αλλαγής στην αντίληψη που αναγνωρίζει ότι θα υπάρξουν επιθέσεις στον κυβερνοχώρο και συνεπώς οι επιχειρήσεις θα πρέπει να είναι κατάλληλα προετοιμασμένες για αυτό το ενδεχόμενο. Σύμφωνα με τα όσα προβλέπει ο Γενικός Κανονισμός Προστασίας Δεδομένων, αποτελεί αδιαπραγμάτευτη ευθύνη της κάθε επιχείρησης να προετοιμαστεί και να μετριάσει τις προκλήσεις που δύναται να προκληθούν από μια επίθεση στον κυβερνοχώρο της, επιστρέφοντας στη συνήθη επιχειρηματική της πρακτική όσο το δυνατόν συντομότερα και παρέχοντας την απαιτούμενη διασφάλιση ότι τα προσωπικά δεδομένα των χρηστών δεν απειλούνται από εγγενείς κινδύνους.

Κεφάλαιο τρίτο

Κίνδυνοι στο Κυβερνοχώρο

Στο τρίτο κεφάλαιο της εργασίας θα γίνει προσπάθεια να αναλυθεί η θεματολογία περί των κινδύνων του κυβερνοχώρου. Ειδικότερα, θα επιχειρηθεί να παρουσιαστεί η έννοια του κινδύνου με σκοπό να περιγραφεί το κόστος αυτού στις επιχειρήσεις και τους οργανισμούς. Το κυρίως μέρος του παρόντος κεφαλαίου ασχολείται με την διαχείριση των κινδύνων του κυβερνοχώρου, σε μια προσπάθεια να παρουσιαστούν τα μέτρα και οι διαδικασίες που προτείνονται από την παγκόσμια βιβλιογραφία επί του θέματος.

3.1 Ορισμός του Κινδύνου

Για να είναι δυνατή η κατανόηση του κινδύνου στο Κυβερνοχώρο (Cyber Risk), κρίνεται σκόπιμο να αναλυθεί η έννοια του κινδύνου. Σαφές είναι ότι η προσπάθεια οργάνωσης σχεδίων για το μέλλον, τόσο από τα μεμονωμένα άτομα όσο και από μια επιχείρηση, εμπεριέχει και βασίζεται σε ένα σύνολο παραγόντων, εναλλακτικών καταστάσεων μεταξύ τους, τα οποία μπορούν να χαρακτηριστούν ως αβέβαια. Ο παράγοντας που μπορεί να προκαλέσει σε δεδομένη μελλοντική περίοδο την εμφάνιση εναλλακτικών καταστάσεων και να επιφέρει αβεβαιότητα (uncertainty) καλείται κίνδυνος (risk). Σύμφωνα με τον Ελευθεριάδη (2018), *«ο κίνδυνος είναι μια από τις παραμέτρους της καθημερινής μας ζωής και επηρεάζει σχεδόν το σύνολο των δραστηριοτήτων των οικονομικών μονάδων, ενώ παράλληλα υπάρχει σε όλες εκείνες τις περιπτώσεις στις οποίες δεν είναι δυνατό να προβλέψουμε με βεβαιότητα το αποτέλεσμα μιας δραστηριότητας».* Η κάθε επιχειρηματική δραστηριότητα, θα ήταν ωφέλιμο να προσδιορίζει το κίνδυνο που συνοδεύει την υλοποίηση αυτής, ενώ παράλληλα θα ήταν σωτήριο να προσδιοριστούν τα μέτρα που πρέπει να ληφθούν στη περίπτωση εμφάνισης του κινδύνου, με σκοπό την αποτελεσματικότερη διαχείριση του. Η εξεύρεση του κινδύνου, όπως υποστηρίζει ο Ελευθερουδάκης Ι (2018), είναι δυνατόν να χρησιμοποιηθεί για να περιγράψει την αβεβαιότητα που συνδέεται με τους παράγοντες, τις διαδικασίες και τα αποτελέσματα τους, οι οποίες μπορεί να έχουν σημαντικές επιπτώσεις, που μπορούν να χαρακτηριστούν ως θετικές

ή ως αρνητικές στην α) Λειτουργική απόδοση της επιχείρησης, β) Την επίτευξη των σκοπών και των στόχων και γ) Την εκπλήρωση των προσδοκιών των μετόχων.

Ο κίνδυνος πάλι όπως αναφέρεται στο ISO-IEC Guide 73, μπορεί να ορισθεί ο συνδυασμός της πιθανότητας ενός γεγονότος και των συνεπειών του. Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος (upside) ή απειλές της επιτυχίας (downside). Συνεπώς, ο κίνδυνος είναι η αβεβαιότητα της μελλοντικής έκβασης ενός γεγονότος. Συμπερασματικά, μπορούμε να πούμε πως ο κίνδυνος είναι ένα γεγονός που επρόκειτο να συμβεί στο μέλλον και δε μπορεί να προβλεφθεί ακριβώς στο παρόν, καθώς υπάρχει μεγάλη αβεβαιότητα. Βέβαια, σημαντικό είναι να τονισθεί ότι ο κίνδυνος υφίσταται όταν το τυχαίο αυτό γεγονός θα επιδράσει αρνητικά στην πιθανότητα της πραγματοποίησης ενός εφικτού στόχου. Από μαθηματικής απόψεως, ο κίνδυνος μπορεί να εκφρασθεί σαν το αποτέλεσμα της πιθανότητας των περιστατικών και των συνεπειών της απώλειας που προκλήθηκε από τον κίνδυνο. Οι καταστάσεις αβεβαιότητας προκύπτουν, όταν υπάρχει μια άγνωστη, απροσδιόριστη κατανομή πιθανότητας στο σύνολο των πιθανών εκβάσεων.

Η αβεβαιότητα σε αυτό το πλαίσιο έχει δύο πιθανές διαστάσεις:

- ✓ Το εύρος των πιθανών εκβάσεων ενός γεγονότος ή μιας δράσης το οποίο μπορεί να είναι στενό, περιορισμένο ή άγνωστο.
- ✓ Την πιθανότητα εμφάνισης μιας έκβασης. Σε μερικές περιπτώσεις αυτό είναι σχετικά εύκολο να καθοριστεί. Σε πολλές άλλες περιπτώσεις μπορεί να μην είναι δυνατό να υπολογιστεί μια πιθανότητα ακριβώς. Η ακόμη και να μην είναι δυνατό να υπολογιστεί μια πιθανότητα καθόλου.

3.2 Κίνδυνοι στο Κυβερνοχώρο

Σύμφωνα με τον Ελευθεριάδη (2018), οι σημερινοί ταχύτατοι ρυθμοί σχεδιασμού, παραγωγής και διάθεσης προϊόντων και υπηρεσιών καθώς και η τεράστια εξάρτηση κάθε δραστηριότητας από περίπλοκα συστήματα υψηλής τεχνολογίας, δημιούργησαν νέους κινδύνους, οι οποίοι είναι δύσκολο να αντιμετωπισθούν. Οι κίνδυνοι που είναι πιθανό να προκύψουν από τη διαχείριση δεδομένων εξαρτώνται από τομείς όπως οι τηλεπικοινωνίες, η ενέργεια, ο κακός χειρισμός του λογισμικού και οι φυσικές καταστροφές. Η ασφάλεια των πληροφοριακών συστημάτων αναφέρεται στην προστασία δεδομένων που αποθηκεύονται, έχουν υποστεί επεξεργασία ή μεταφερθεί σε μηχανογραφικά κέντρα ή προσωπικούς υπολογιστές. Οι κίνδυνοι των πληροφοριακών συστημάτων μπορούν να συνοψισθούν σε τέσσερα σημεία:

- ✓ Ο κίνδυνος ζημιάς στο τεχνικό μέρος των συστημάτων και στον χώρο εγκατάστασης των συστημάτων, από φυσική καταστροφή, πυρκαγιά, κλιματολογικές συνθήκες, τρομοκρατικές ενέργειες κ.α.
- ✓ Ο κίνδυνος από τις διαδικασίες επεξεργασίας δεδομένων.
- ✓ Ο κίνδυνος απώλειας δεδομένων ή εμφάνισης των δεδομένων σε μη εξουσιοδοτημένα άτομα.
- ✓ Ο κίνδυνος ακούσιας αλλοίωσης των δεδομένων λόγω ενός τεχνικού προβλήματος.
- ✓ Ο κίνδυνος εκούσιας αλλοίωσης δεδομένων από μη εξουσιοδοτημένα άτομα.

Ο όρος κίνδυνος στον κυβερνοχώρο (cyber risk) έχει αποτελέσει αντικείμενο έρευνας πολλών ερευνητικών ομάδων και έχει συμπεριληφθεί σε πολλά άρθρα τόσο της ελληνικής όσο και της ξενόγλωσσης βιβλιογραφίας. Βέβαια, σημαντικό είναι να αναφερθεί ότι η πλειονότητα των ερευνών προβάλλουν το θέμα αυτό με μια συγκεκριμένη σκοπιά και προοπτική. Με βάση την ανασκόπηση της βιβλιογραφίας που περιγράφεται στο κεφάλαιο αυτό, διαπιστώνουμε ότι ο όρος χρησιμοποιείται ευρέως και οι ορισμοί του είναι μεταβαλλόμενοι και συνδεδεμένοι με το περιβάλλον, συχνά υποκειμενικοί και, κατά καιρούς, μη επαρκώς ενημερωμένοι. Η διαθέσιμη

βιβλιογραφία για το συγκεκριμένο όρο είναι περιορισμένη και αναπτύσσεται σε συγκεκριμένα πλαίσια.

Προσπαθώντας να παρουσιαστεί ένας ευρύτερα αποδεκτός ορισμός ευθυγραμμισμένος με τον αληθινό διεπιστημονικό χαρακτήρα του κινδύνου στο κυβερνοχώρο, αναθεωρήθηκε η σχετική βιβλιογραφία για να προσδιοριστεί το φάσμα των ορισμών, με σκοπό να διακριθούν κυρίαρχα θέματα και να διακριθούν πτυχές του κινδύνου στο κυβερνοχώρο.

Η ανασκόπηση της βιβλιογραφίας περιελάμβανε ένα ευρύ φάσμα πηγών, συμπεριλαμβανομένου ενός ευρέος φάσματος ακαδημαϊκών κλάδων, όπως: πληροφορική, μηχανική, πολιτικές σπουδές, ψυχολογία, μελέτες ασφάλειας, διαχείριση, εκπαίδευση και κοινωνιολογία. Οι πιο συνηθισμένοι κλάδοι που καλύπτονται στην ανασκόπηση της παρούσας βιβλιογραφίας είναι η μηχανική, η τεχνολογία, η επιστήμη των υπολογιστών. Αλλά, σε πολύ μικρότερο βαθμό, υπήρχαν επίσης στοιχεία για το θέμα του κινδύνου στον κυβερνοχώρο σε άρθρα σχετικά με το δίκαιο, την υγειονομική περίθαλψη, τη δημόσια διοίκηση, τη λογιστική, τη διαχείριση, την κοινωνιολογία, την ψυχολογία και την εκπαίδευση.

Σύμφωνα με τα όσα αναφέρουν οι Eling και Wirfs (2016), ο κυβερνοχώρος νοείται ως ο διαδραστικός τομέας που αποτελείται από όλα τα ψηφιακά δίκτυα που χρησιμοποιούνται για την αποθήκευση, την τροποποίηση και την επικοινωνία των πληροφοριών και περιλαμβάνει όλα τα πληροφοριακά συστήματα που χρησιμοποιούνται για την υποστήριξη των επιχειρήσεων, των υποδομών και των υπηρεσιών που παρέχονται μέσω αυτών. Συνεχίζοντας, ορίζουν τους κινδύνους του κυβερνοχώρου, ως λειτουργικούς κινδύνους που σχετίζονται με τα περιουσιακά στοιχεία πληροφορικής και τεχνολογίας που έχουν συνέπειες που επηρεάζουν την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των πληροφοριών και των πληροφοριακών συστημάτων ενός μεμονωμένου χρήστη ή οργανισμού.

Οι Mukhopadhyay et al. (2005), ορίζουν τους κινδύνους του κυβερνοχώρου ως τον κίνδυνο που σχετίζεται με κακόβουλες ηλεκτρονικές πράξεις που προκαλούν διαταραχές στις επιχειρήσεις, καθώς και οικονομικές απώλειες. Οι Böhme και Kataria (2006), αναφέρουν ότι είναι οι υπαίτιοι για τα προβλήματα στα πληροφοριακά συστήματα – προσδιορίζοντάς τους έτσι μέσω των συνεπειών που των αποτελεσμάτων που επιφέρουν.

Τέλος, οι Ögüt et al. (2011), τους ορίζουν, επιγραμματικά, ως τους κινδύνους των πληροφοριακών συστημάτων.

3.3 Κυβερνοχώρο στο χώρο εστίασης

Δεδομένου ότι η χρήση της τεχνολογίας αυτοματισμού είναι αποδοτική ως προς το κόστος, εφαρμόζεται κατά κόρον από μια πλειάδα επιχειρήσεων, δίνοντας σημαντικά οφέλη. Τα οφέλη όμως αυτά που παρέχουν τα συστήματα αυτοματισμού συνοδεύονται από ένα σύνολο τρωτών σημείων, που μπορεί να έχουν σημαντικές επιπτώσεις ακόμα και στη λειτουργία της ίδιας της επιχείρησης

Τα τελευταία χρόνια γίνεται συχνά λόγος για τους Κινδύνους στο Κυβερνοχώρο, όπου επηρεάζουν κάθε επιχείρηση ανεξάρτητα από το κλάδο στον οποίο δραστηριοποιείται. Με πολλούς τρόπους, οι κίνδυνοι από τις απειλές στον κυβερνοχώρο δεν διαφέρουν από τους κινδύνους για την ασφάλεια που αντιμετωπίζουν οι εταιρείες τροφίμων καθημερινά.

Οι κίνδυνοι για την ασφάλεια των δεδομένων στις εταιρείες τροφίμων εμπίπτουν σε ορισμένες κατηγορίες, όπως κλοπή, έκθεση του κοινού, διαφθορά ή απώλεια δεδομένων και χειραγώγηση ή παραποίηση δεδομένων. Η αξιολόγηση της πιθανότητας επίθεσης σε κάθε κατηγορία απαιτεί στον εντοπισμό κακόβουλων παραγόντων και τον τρόπο με τον οποίο ο καθένας μπορεί να επωφεληθεί από μια επίθεση.

Ο κίνδυνος για τον τομέα των τροφίμων είναι, δυστυχώς, ολοένα και πιο έντονος. Τον Μάιο του 2017, περίπου 200.000 εταιρείες, συμπεριλαμβανομένου και επιχειρήσεων τροφίμων αλλά και ποτών σε όλο τον κόσμο, επηρεάστηκαν από τις επιθέσεις στο κυβερνοχώρο.

Συχνά, η διείσδυση στον κυβερνοχώρο αποτελεί έναν τρόπο για την κλοπή στοιχείων πιστωτικής κάρτας ή οποιαδήποτε άλλη μορφή παραβίασης των δεδομένων. Επίσης, η «Agroterrorism», αποτελεί κίνδυνο, όπου οι χειριστές του, προσπαθούν να ακτινοβολούν ή να μολύνουν τα τρόφιμα αποκτώντας τον έλεγχο του αυτοματοποιημένου εξοπλισμού, γεγονός που αποτελεί μια αυξανόμενη απειλή, καθώς τα συστήματα γίνονται πιο περίπλοκα. Εάν ένας υπάλληλος μπορεί να συνδεθεί από το σπίτι, τότε μπορεί και ο καθένας με μεγάλη ευκολία να ελέγχει ένα σύστημα από οπουδήποτε.

Στην πραγματικότητα, ο τομέας τροφίμων και ποτών είναι ο πλέον στοχευμένος για επιθέσεις στον κυβερνοχώρο μετά τη λιανική πώληση. Σύμφωνα με την Trustware Global Security, μόλις οι μισές από τις επιθέσεις είναι ενάντια στη Λιανική πώληση και περίπου το ένα τέταρτο είναι κατά των Τροφίμων. Αξίζει να σημειωθεί ότι για πολλές μεγάλες επιχειρήσεις η επιχείρησή τους μπορεί να διασχίσει και τους δύο τομείς με συστήματα και τεχνολογία που συνδέονται μεταξύ τους.

Η απειλή επιθέσεων στον κυβερνοχώρο δεν περιορίζεται μόνο στις μεγάλες βιομηχανίες, αλλά μπορεί να επηρεάσει και τις μικρότερες επιχειρήσεις με σημαντικές επιπτώσεις, ιδίως οικονομικές.

Για όλες τις επιχειρήσεις, η απώλεια της εμπιστοσύνης των πελατών, το κόστος από τη διακοπή παραγωγής και η αλλοίωση του προϊόντος μπορούν να προκύψουν από επιθέσεις στον κυβερνοχώρο και εάν η επίθεση οδηγήσει σε βλάβη που προκαλείται στους καταναλωτές από τα μολυσμένα προϊόντα, τότε η ζημιά που θα έχει η εταιρεία θα μεγεθυνθεί , με σημαντική οικονομική καταστροφή.

Κεφάλαιο τέταρτο

Μεθοδολογία Έρευνας

4.1 Ποσοτική έρευνα

Η έρευνα αφορά στις αντιλήψεις των επιχειρηματιών του ελληνικού κλάδου της εστίασης (κλάδος ποτών και τροφίμων) για την διασφάλιση των πληροφοριών από τους κινδύνους του κυβερνοχώρου.

Ο σκοπός της παρούσας έρευνας είναι η δημιουργία μιας αναλυτικής και συστηματικής καταγραφής των θεμάτων που προκύπτουν από τις παρατηρήσεις των συμμετεχόντων στο κομμάτι της διασφάλισης πληροφοριών της κάθε εταιρίας. Ο κύριος στόχος της συγκεκριμένης ποσοτικής έρευνας είναι να παρουσιάσει τα αποτελέσματα κάθε ερώτησης σχετικά με τη συμπεριφορά των επιχειρηματιών, καθώς και τα περιγραφικά στατιστικά μέτρα που προκύπτουν από κάθε μία ερώτηση ξεχωριστά. Τα περιγραφικά μέτρα που θα εξεταστούν έχουν αριθμητική μορφή και αποτελούνται από στατιστικά στοιχεία, ποσοστά και άλλα μέτρα.

4.2 Περιγραφή Ερωτηματολογίου

Το ερωτηματολόγιο που δόθηκε αποτελείται από 9 κλειστές ερωτήσεις, όπου είναι βασισμένες σε κλίμακα Likert. Πιο συγκεκριμένα, χρησιμοποιήθηκε διάταξη των ερωτήσεων, βασισμένες στην ψυχολογία των ερωτώμενων σχετικά με την ασφάλεια πληροφοριών των εταιριών. Οι ερωτήσεις είναι αρχικά γενικότερες και ύστερα περισσότερο ειδικές και πιο επικεντρωμένες στο ζητούμενο θέμα.

Αρχικά, οι ερωτήσεις αποσκοπούν στη καταγραφή της γνώσης κινδύνου που έχουν οι επιχειρηματίες ως προς την ασφάλεια πληροφοριών. Τίθεται το ερώτημα για το αν γνωρίζουν αυτούς τους κινδύνους και στη συνέχεια γίνεται αναφορά στο κόστος παραβίασης τους καθώς και της διαρροής τους.

Τέλος γίνεται μία αναφορά στους κανονισμούς ασφάλειας των πληροφοριών και στις διαδικασίες που τις διέπουν. Παρατηρείται λοιπόν μία κλιμάκωση ως προς

την διατύπβση των ερωτήσεων. Επίσης, υπάρχει ισχυρή συνοχή μεταξύ των ερωτήσεων, ώστε οι ερωτώμενοι να μπορούν να απαντούν άμεσα και με ευκολία.

4.3 Δείγμα

Είναι γνωστό ότι το δείγμα είναι ένα υποσύνολο του πληθυσμού που θα μελετηθεί, το οποίο επιλέγεται με συγκεκριμένες μεθόδους. Αποτελείται ουσιαστικά από μία ομάδα ανθρώπων που λαμβάνονται από σχετικά μεγάλο πληθυσμό. Στην παρούσα έρευνα το δείγμα αποτελείται από λίγα άτομα, πιο συγκεκριμένα από 21 επιχειρηματίες από τον κλάδο της εστίασης. Το μικρό μέγεθος του δείγματος επηρεάζει την αντιπροσωπευτικότατά του.

4.4 Δειγματοληψία

Η επιλογή του δείγματος γίνεται με κριτήριο την ευκολία συλλογής δεδομένων από το δείγμα. Η δειγματοληψία που επιλέχτηκε για την έρευνα είναι εκείνη της ευκολίας (convenience sample). Η διαδικασία της επιλογής του δείγματος αφορά αρχικά τα άτομα τα οποία θα ήταν πιο πλησιέστερα και εύκαιρα στην παρούσα φάση, ώστε να ολοκληρώσουν το ερωτηματολόγιο. Η διαδικασία συνεχίζεται μέχρι να βρεθεί το απαιτούμενο μέγεθος για την κάλυψη του ερωτηματολογίου. Θεωρείται η πιο άμεση μέθοδος για την εύρεση κατάλληλου δείγματος.

4.5 Τρόπος Ανάλυσης Αποτελεσμάτων

Σε πρώτη φάση ακολουθήθηκαν κάποια βήματα προκειμένου να επιτευχθεί η περιγραφική στατιστική για κάθε ερώτηση ξεχωριστά με εφαρμογή των κατάλληλων μεθόδων. Συνολικά πραγματοποιήθηκαν 21 ερωτηματολόγια που περιείχαν 9 κλειστές ρωτήσεις .Η κλίμακα των ερωτήσεων ξεκινούσε από το 1=ΚΑΘΟΛΟΥ και κατέληγε στο 5=ΠΑΡΑ ΠΟΛΥ.

Στη συνέχεια έγινε εισαγωγή των δεδομένων στο στατιστικό λογισμικό SPSS (Statistical Package for Social Sciences), ώστε να είναι δυνατή η επεξεργασίας τους για την ανάλυση.

Ως προς την καταγραφή των απαντήσεων στις ερωτήσεις δημιουργήθηκε πίνακας δεδομένων, ο οποίος αποτελείται από γραμμές, όπου αντιστοιχούνται οι ερωτώμενοι και στήλες, όπου αντιστοιχούνται οι ερωτήσεις. Οι απαντήσεις των ερωτήσεων καταγράφηκαν στο λογισμικό με τη μορφή αριθμών και επεξεργάστηκαν

ως προς την μεταβλητή τους. Συγκεκριμένα, και για τις 9 ερωτήσεις ορίστηκε η μεταβλητή “Ordinal”,η οποία αντιπροσωπεύει την διάταξη των αποτελεσμάτων των ερωτήσεων.

Για τα περιγραφικά στατιστικά μέτρα ακολουθήθηκαν τα απαραίτητα βήματα στο στατιστικό λογισμικό του SPSS.Αρχικά γίνεται ανάλυση αποτελεσμάτων σχετικά με την μέση τιμή, την διάμεσο και την τυπική απόκλιση κάθε ερώτησης. Επίσης, παρουσιάζονται οι πίνακες με τις συχνότητες και τα ποσοστά κάθε ερώτησης. Όλα τα παραπάνω παρουσιάζονται εκτενέστερα στη συνέχεια της εργασίας στο Κεφάλαιο 5.

4.6 Ανάλυση Αποτελεσμάτων

Συλλέγοντας τις απαντήσεις των ερωτηματολογίων από το δείγμα των 21 ατόμων και έχοντας περάσει τα δεδομένα στο στατιστικό πρόγραμμα SPSS, εφαρμόστηκε περιγραφική στατιστική. Παρακάτω παρουσιάζονται η μέση τιμή, η διάμεσος και η τυπική απόκλιση και των 9 ερωτήσεων.

Πίνακας 4.1.Συνολικός πίνακας για την μέση τιμή,διάμεσο και τυπική απόκλιση.

	Γνωρίζω για δυνητικούς κινδύνους όσο αφορά στην ασφάλεια πληροφοριών	Έχω αρκετή γνώση όσο αφορά το κόστος παραβίασης ασφάλειας πληροφοριών	Αντιλαμβάνομαι τον κίνδυνο της διαρροής ασφάλειας πληροφοριών	Ενημερώνομαι όσο αφορά στην ασφάλεια πληροφοριών	Μοιράζομαι όσα ξέρω για την ασφάλεια πληροφοριών για να ενισχύσω τη γνώση μου	Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν είναι σημαντικοί για την εταιρία μου	Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν επηρεάζουν τη συμπεριφορά μου	Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν, έχουν εφιστήσει την προσοχή μου	Σωστή συμπεριφορά για κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι σημαντικές για την εταιρία
Μέση τιμή	2.86	2.29	3.62	2.33	3.52	3.71	3.71	2.76	4.19
Διάμεσος	3.00	2.00	4.00	2.00	4.00	4.00	4.00	2.00	5.00
Τυπική απόκλιση	1.195	1.309	1.396	1.426	1.289	1.488	1.384	1.480	1.167

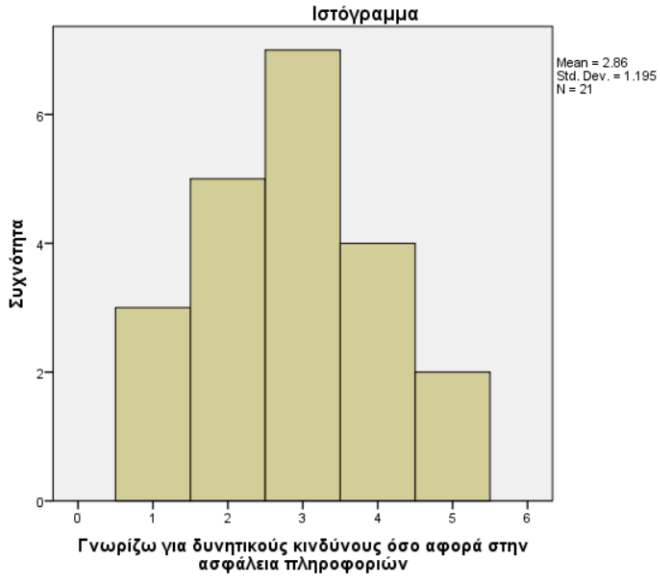
<u>Ερώτηση 1η : Γνωρίζω για δυνητικούς κινδύνους όσο αφορά στην ασφάλεια πληροφοριών.</u>

Πίνακας 4.2.Πίνακας συχνοτήτων και τα ποσοστά.

		Συχνότητα	Ποσοστό
	Καθόλου	3	14.3
	Λίγο	5	23.8
	Ούτε λίγο ούτε πολύ	7	33.3
	Πολύ	4	19.0
	Πάρα πολύ	2	9.5
	Συνολικά	21	100.0

Πίνακας 4.3. Περιγραφικά μέτρα.

Μέση τιμή	2.86
Διάμεσος	3.00
Τυπική απόκλιση	1.195



Γράφημα 1.Γνωρίζω για δυνητικούς κίνδυνος όσο αφορά στην ασφάλεια πληροφοριών.

Στον πρώτο πίνακα, στην στήλη Frequency,η οποία αποτελείται από τις συχνότητες των δεδομένων, παρατηρείται ότι τα 3 από τα 21 άτομα που ερωτήθηκαν στην συγκεκριμένη ερώτηση απάντησαν ότι δεν γνωρίζουν καθόλου για δυνητικούς κινδύνους όσο αφορά στην ασφάλεια πληροφοριών. Αντίστοιχα, 5 από τα 21 απάντησαν ότι γνωρίζουν λίγο,7 άτομα αντίστοιχα δε γνώριζαν ούτε λίγο ούτε πολύ, 4 άτομα απάντησαν ότι γνώριζαν πολύ και τέλος μόνο 2 απάντησαν ότι γνώριζαν πάρα πολύ.

Αντίστοιχα, στην στήλη Percent παρουσιάζονται τα ποσοστά των συχνοτήτων. Ουσιαστικά το 14,3% των ατόμων δεν γνωρίζει καθόλου, το 23,8% γνωρίζει λίγο, το 33,3% δε γνωρίζει ούτε λίγο ούτε πολύ, το 19% γνωρίζει πολύ ενώ το 9,5% γνωρίζει πάρα πολύ για δυνητικούς κινδύνους.

Στον επόμενο πίνακα παρατηρείται ότι η μέση τιμή των δεδομένων είναι 2,86, όπου βγαίνει το συμπέρασμα ότι ο μέσος όρος των ατόμων που γνωρίζουν είναι ούτε λίγο ούτε πολύ, διότι προσεγγίζει την κατηγοριοποίηση 3. Επίσης, η τυπική απόκλιση είναι 1,195, όπου αντιπροσωπεύει το πόσο διεσπαρμένες είναι οι μεταβλητές από τον μέσο όρο. Παρουσιάζεται το ιστόγραμμα με τις συχνότητες.

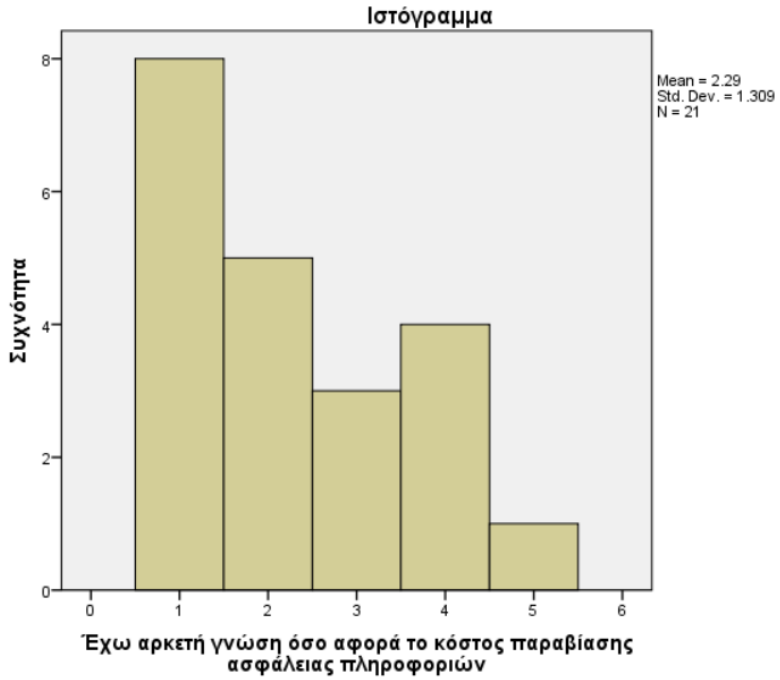
Ερώτηση 2η: Έχω αρκετή γνώση όσο αφορά το κόστος παραβίασης ασφάλειας πληροφοριών.

Πίνακας 4.4.Πίνακας συχνοτήτων και τα ποσοστά.

	Συχνότητα	Ποσοστό
Καθόλου	8	38.1
Λίγο	5	23.8
Ούτε λίγο ούτε πολύ	3	14.3
Πολύ	4	19.0
Πάρα πολύ	1	4.8
Συνολικά	21	100.0

Πίνακας 4.5. Περιγραφικά μέτρα.

Μέση τιμή	2.29
Διάμεσος	2.00
Τυπική απόκλιση	1.309



Γράφημα 2.Έχω αρκετή γνώση όσο αφορά το κόστος παραβίασης ασφάλειας πληροφοριών.

Παρατηρείται ότι τα 8 από τα 21 άτομα, που ερωτήθηκαν στην ερώτηση σχετικά με το αν έχουν αρκετή γνώση όσο αφορά το κόστος παραβίασης ασφάλειας πληροφοριών, απάντησαν ότι δεν έχουν καθόλου γνώση. Αντίστοιχα, 5 άτομα απάντησαν ότι έχουν λίγη γνώση, 3 άτομα απάντησαν ότι δεν έχουν ούτε λίγη ούτε πολύ, 4 άτομα απάντησαν ότι έχουν πολύ γνώση και τέλος μόνο 1 άτομο απάντησε ότι έχει πάρα πολύ γνώση.

Τα ποσοστά των συχνοτήτων δείχνουν ότι το 38,1% των ατόμων δεν έχει καθόλου γνώση, το 23,8% έχει λίγη γνώση, το 14,3% δεν έχει ούτε λίγο ούτε πολύ γνώση, το 19% έχει πολύ γνώση ενώ το 4,8% έχει πάρα πολύ γνώση για το θέμα.

Παρακάτω παρατηρείται ότι η μέση τιμή των δεδομένων είναι 2,29, άρα ο μέσος όρος των ατόμων δείχνει ότι έχουν λίγη γνώση, διότι προσεγγίζει την κατηγοριοποίηση 2. Επίσης, η τυπική απόκλιση είναι 1,309.Παρουσιάζεται το ιστόγραμμα.

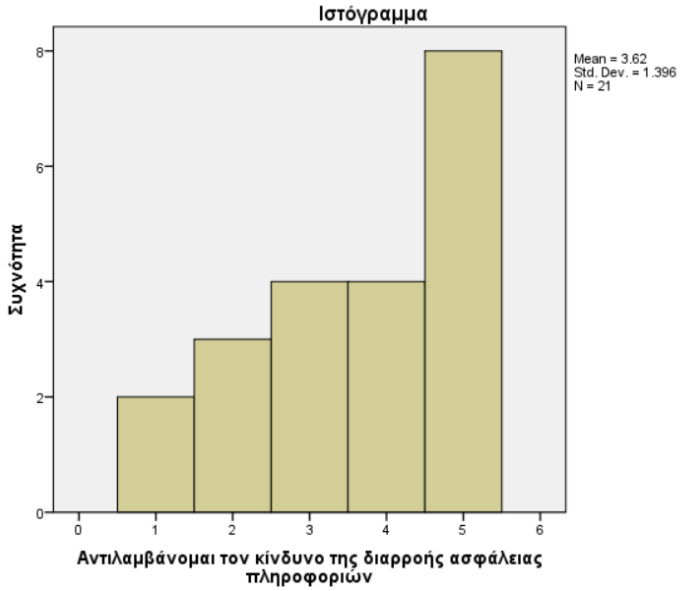
Ερώτηση 3η: Αντιλαμβάνομαι τον κίνδυνο της διαρροής ασφάλειας πληροφοριών.

Πίνακας 4.6.Πίνακας συχνοτήτων και τα ποσοστά.

	Συχνότητα	Ποσοστό
Καθόλου	2	9.5
Λίγο	3	14.3
Ούτε λίγο ούτε πολύ	4	19.0
Πολύ	4	19.0
Πάρα πολύ	8	38.1
Συνολικά	21	100.0

Πίνακας 4.7. Περιγραφικά μέτρα.

Μέση τιμή	3.62
Διάμεσος	4.00
Τυπική απόκλιση	1.396



Γράφημα 3.Αντιλαμβάνομαι τον κίνδυνο της διαρροής ασφάλειας πληροφοριών.

Παρατηρείται ότι τα 2 από τα 21 άτομα, που ερωτήθηκαν στην ερώτηση σχετικά με το αν αντιλαμβάνονται τον κίνδυνο της διαρροής ασφάλειας πληροφοριών, απάντησαν ότι δεν τον αντιλαμβάνονται καθόλου. Αντίστοιχα, 3 άτομα απάντησαν ότι αντιλαμβάνονται τον κίνδυνο λίγο, 4 άτομα δεν τον αντιλαμβάνονται ούτε λίγο ούτε πολύ, άλλα 4 άτομα τον αντιλαμβάνονται πολύ και τέλος 8 άτομα πάρα πολύ.

Αντίστοιχα, αναφορικά με τα ποσοστά αναφέρεται ότι το 9,5% των ατόμων δεν αντιλαμβάνεται καθόλου τον κίνδυνο, το 14,3% λίγο, το 19% ούτε λίγο ούτε πολύ, το άλλο 19% πολύ ενώ το 38,1% πάρα πολύ.

Ύστερα, παρατηρείται ότι η μέση τιμή των δεδομένων είναι 3,62, άρα ο μέσος όρος των ατόμων δείχνει ότι αντιλαμβάνονται πολύ τον κίνδυνο, διότι προσεγγίζει την κατηγοριοποίηση 4.

Επίσης, η τυπική απόκλιση είναι 1,396. Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

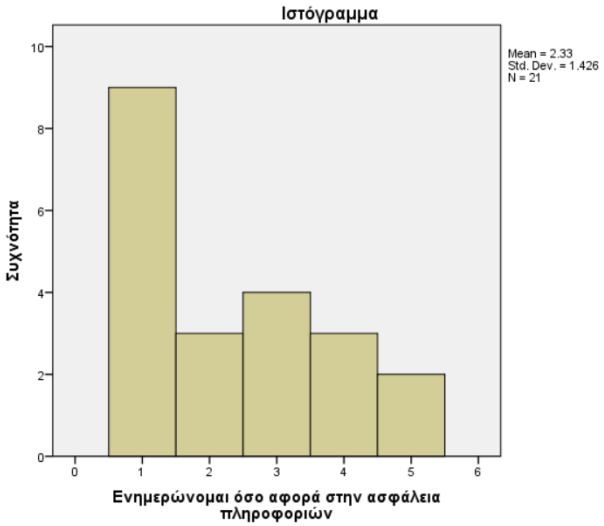
Ερώτηση 4η: Ενημερώνομαι όσο αφορά στην ασφάλεια πληροφοριών.

Πίνακας 4.8.Πίνακας συχνοτήτων και τα ποσοστά.

	Συχνότητα	Ποσοστό
Καθόλου	9	42.9
Λίγο	3	14.3
Ούτε λίγο ούτε πολύ	4	19.0
Πολύ	3	14.3
Πάρα πολύ	2	9.5
Συνολικά	21	100.0

Πίνακας 4.9. Περιγραφικά μέτρα.

Μέση τιμή	2.33
Διάμεσος	2.00
Τυπική απόκλιση	1.426



Γράφημα 4.Ενημερώνομαι όσο αφορά στην ασφάλεια πληροφοριών.

Τα 9 από τα 21 άτομα, απάντησαν ότι δεν ενημερώνονται καθόλου όσον αφορά στην ασφάλεια πληροφοριών. Αντίστοιχα, 3 άτομα απάντησαν ότι ενημερώνονται λίγο, 4 άτομα ούτε λίγο ούτε πολύ, 3 άτομα πολύ και 2 άτομα πάρα πολύ.

Τα ποσοστά των συχνοτήτων δείχνουν ότι το 42,9% των ατόμων δεν ενημερώνεται καθόλου όσο αφορά στην ασφάλεια πληροφοριών, το 14,3% λίγο, το 19% ούτε λίγο ούτε πολύ, το 14,3% πολύ ενώ το 9,5% πάρα πολύ.

Η μέση τιμή των δεδομένων είναι 2,33, άρα ο μέσος όρος των ατόμων ενημερώνεται λίγο. Η τυπική απόκλιση είναι 1,426. Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

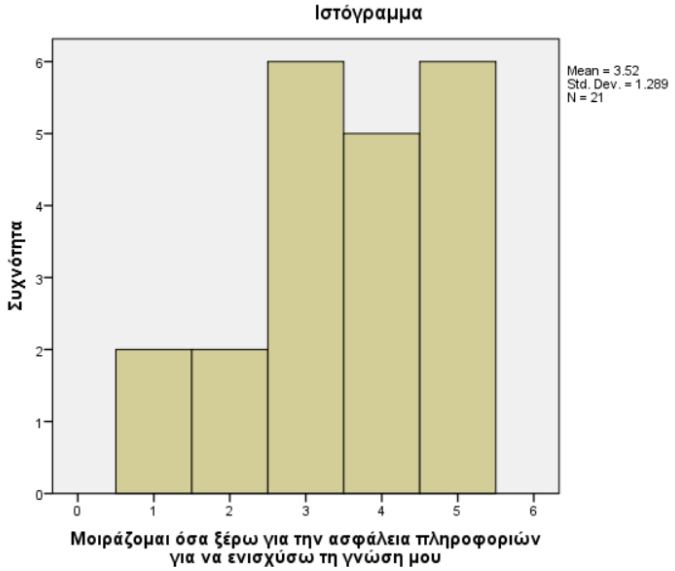
<u>Ερώτηση 5η: Μοιράζομαι όσα ξέρω για την ασφάλεια πληροφοριών για να ενισχύσω τη γνώση μου.</u>

Πίνακας 4.10.Πίνακας συχνοτήτων και τα ποσοστά.

		Συχνότητα	Ποσοστό
	Καθόλου	2	9.5
	Λίγο	2	9.5
	Ούτε λίγο ούτε πολύ	6	28.6
	Πολύ	5	23.8
	Πάρα πολύ	6	28.6
	Συνολικά	21	100.0

Πίνακας 4.11. Περιγραφικά μέτρα

Μέση τιμή	3.52
Διάμεσος	4.00
Τυπική απόκλιση	1.289



Γράφημα 5.Μοιράζομαι όσα ξέρω για την ασφάλεια πληροφοριών για να ενισχύσω τη γνώση μου.

Αρχικά, παρατηρείται ότι τα 2 άτομα απάντησαν ότι δεν μοιράζεται καθόλου όσα ξέρουν για την ασφάλεια πληροφοριών για να ενισχύσουν τη γνώση τους. Αντίστοιχα 2 άτομα σε αυτή την ερώτηση απάντησαν λίγο, 6 άτομα απάντησαν ούτε λίγο ούτε πολύ, 5 άτομα απάντησαν πολύ και 6 άτομα απάντησαν πάρα πολύ.

Τα ποσοστά των συχνοτήτων δείχνουν ότι το 9,5% των ατόμων δεν μοιράζεται καθόλου όσα ξέρει για την ασφάλεια πληροφοριών για να ενισχύσει τη γνώση του, άλλο ένα 9,5% λίγο, το 28,6% ούτε λίγο ούτε πολύ, το 23,8% πολύ ενώ το 28,6% πάρα πολύ.

Η μέση τιμή των δεδομένων είναι 3,52, άρα ο μέσος όρος των ατόμων μοιράζεται πολύ. Η τυπική απόκλιση είναι 1,289.Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

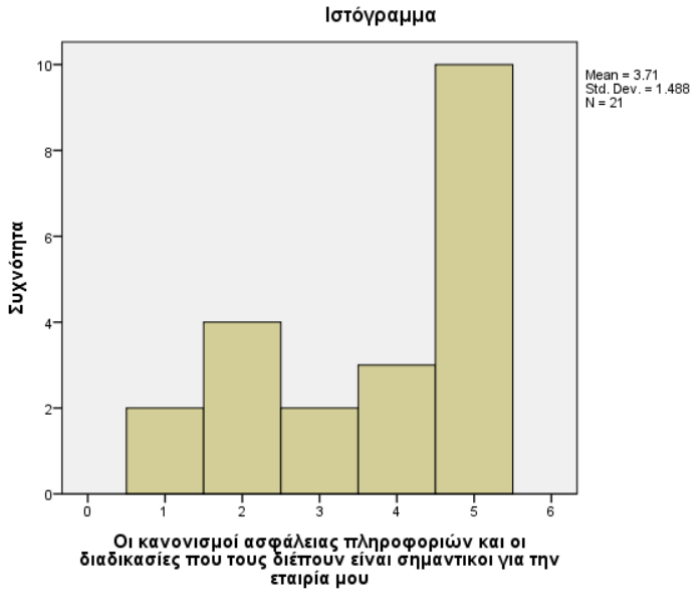
<u>Ερώτηση 6η: Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν είναι σημαντικοί για την εταιρία μου.</u>

Πίνακας 4.12.Πίνακας συχνοτήτων και τα ποσοστά.

	Συχνότητα	Ποσοστά
Καθόλου	2	9.5
Λίγο	4	19.0
Ούτε λίγο ούτε πολύ	2	9.5
Πολύ	3	14.3
Πάρα πολύ	10	47.6
Συνολικά	21	100.0

Πίνακας 4.13. Περιγραφικά μέτρα.

Μέση τιμή	3.71
Διάμεσος	4.00
Τυπική απόκλιση	1.488



Γράφημα 6.Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν είναι σημαντικοί για την εταιρία μου.

Παρατηρείται ότι 2 άτομα απάντησαν ότι οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν δεν είναι καθόλου σημαντικοί για την εταιρία τους. Αντίστοιχα, για τα 4 άτομα σε αυτή την ερώτηση απάντησαν λίγο, 2 άτομα απάντησαν ούτε λίγο ούτε πολύ, 3 άτομα απάντησαν πολύ και 10 άτομα απάντησαν πάρα πολύ.

Τα ποσοστά των συχνοτήτων δείχνουν ότι για το 9,5% δεν είναι καθόλου σημαντικοί οι κανονισμοί, για το 19% λίγο, για το 9,5% ούτε λίγο ούτε πολύ, για το 14,3% πολύ ενώ για το 47,6% πάρα πολύ.

Η μέση τιμή των δεδομένων είναι 3,71, άρα ο μέσος όρος των ατόμων πιστεύει ότι είναι πολύ σημαντικοί οι κανονισμοί. Η τυπική απόκλιση είναι 1,289. Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

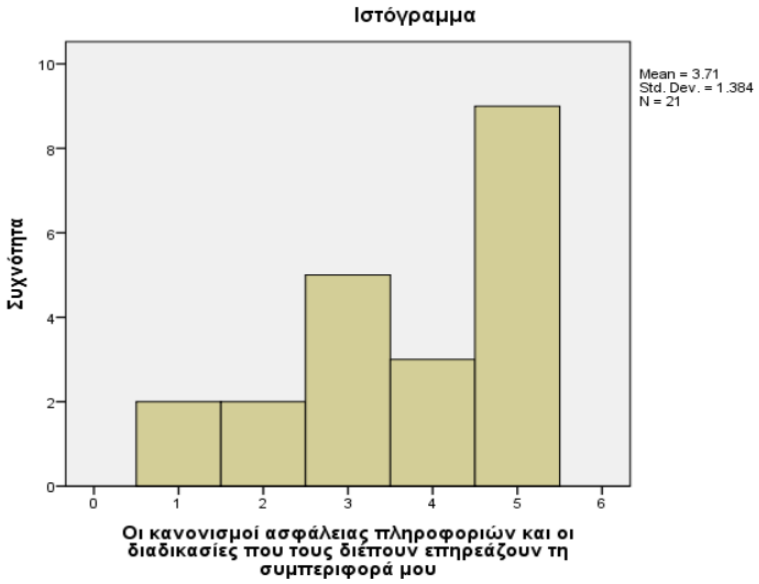
<u>Ερώτηση 7η: Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν επηρεάζουν τη συμπεριφορά μου.</u>

Πίνακας 4.14.Πίνακας συχνοτήτων και τα ποσοστά.

		Συχνότητα	Ποοστό
	Καθόλου	2	9.5
	Λίγο	2	9.5
	Ούτε λίγο ούτε πολύ	5	23.8
	Πολύ	3	14.3
	Πάρα πολύ	9	42.9
	Συνολικά	21	100.0

Πίνακας 4.15. Περιγραφικά μέτρα.

Μέση τιμή	3.71
Διάμεσος	4.00
Τυπική απόκλιση	1.384



Γράφημα 7.Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν επηρεάζουν τη συμπεριφορά μου.

Παρατηρείται ότι 2 άτομα θεωρούν ότι οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν δεν επηρεάζουν καθόλου τη συμπεριφορά τους. Άλλα 2 άτομα απάντησαν ότι επηρεάζουν λίγο τη συμπεριφορά τους, 5 άτομα απάντησαν ούτε λίγο ούτε πολύ, 3 άτομα απάντησαν ότι επηρεάζουν πολύ τη συμπεριφορά τους και 9 άτομα απάντησαν πάρα πολύ.

Τα ποσοστά των συχνοτήτων δείχνουν ότι το 9,5% δεν επηρεάζεται καθόλου, επίσης το 9,5% επηρεάζεται λίγο,το 23,8% ούτε λίγο ούτε πολύ, το 14,3% πολύ ενώ για το 42,9% πάρα πολύ.

Η μέση τιμή των δεδομένων είναι 3,71, άρα ο μέσος όρος των ατόμων επηρεάζεται πολύ από τους κανονισμούς. Η τυπική απόκλιση είναι 1,384. Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

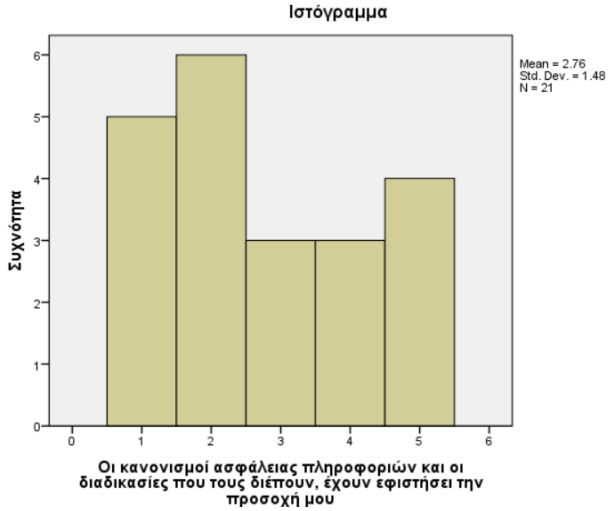
<u>Ερώτηση 8η: Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν, έχουν εφιστήσει την προσοχή μου.</u>

Πίνακας 4.16.Πίνακας συχνοτήτων και τα ποσοστά.

		Συχνότητα	Ποσοστό
	Καθόλου	5	23.8
	Λίγο	6	28.6
	Ούτε λίγο ούτε πολύ	3	14.3
	Πολύ	3	14.3
	Πάρα πολύ	4	19.0
	Συνολικά	21	100.0

Πίνακας 4.17. Περιγραφικά μέτρα.

Μέση τιμή	2.76
Διάμεσος	2.00
Τυπική απόκλιση	1.480



Γράφημα 8.Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν , έχουν εφιστήσει την προσοχή μου.

Παρατηρείται ότι 5 άτομα θεωρούν ότι οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν δεν εφιστούν καθόλου τη προσοχή τους. Επίσης, 6 άτομα θεωρούν λίγο,3 άτομα ούτε λίγο ούτε πολύ, 3 άτομα πολύ και 4 άτομα πάρα πολύ.Τα ποσοστά των συχνοτήτων δείχνουν ότι το 23,8% οι κανονισμοί δεν εφιστούν καθόλου τη προσοχή τους, επίσης το 28,6% λίγο,το 14,3% ούτε λίγο ούτε πολύ,άλλο ένα 14,3% πολύ ενώ το 19% πάρα πολύ.Η μέση τιμή των δεδομένων είναι 2,76.Η τυπική απόκλιση είναι 1,48.Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

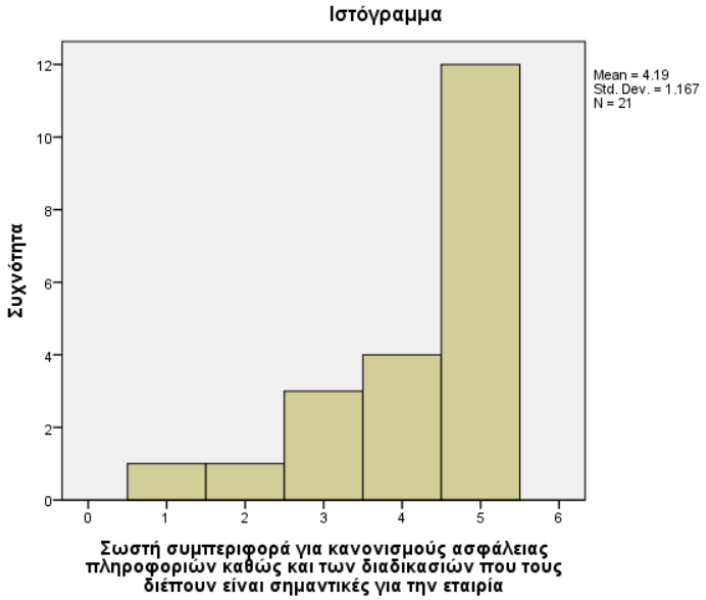
<u>Ερώτηση 9η:Η σωστή συμπεριφορά όσο αφορά τους κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι σημαντικές για την εταιρία μου.</u>

Πίνακας 4.18.Πίνακας συχνοτήτων και τα ποσοστά.

	Συχνότητα	Ποσοστό
Καθόλου	1	4.8
Λίγο	1	4.8
Ούτε λίγο ούτε πολύ	3	14.3
Πολύ	4	19.0
Πάρα πολύ	12	57.1
Συνολικά	21	100.0

Πίνακας 4.19. Περιγραφικά μέτρα.

Μέση τιμή	4.19
Διάμεσος	5.00
Τυπική απόκλιση	1.167



Γράφημα 9.Σωστή συμπεριφορά για κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασίων που τους διέπουν είναι σημαντικές για την εταιρία μου.

Παρατηρείται ότι ένα άτομο δεν θεωρεί καθόλου ότι η σωστή συμπεριφορά όσο αφορά τους κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι σημαντικές για την εταιρία του.

Επίσης άλλο ένα άτομο σε αυτή την ερώτηση απάντησε λίγο ,3 άτομα απάντησαν ούτε λίγο ούτε πολύ, 4 άτομα απάντησαν πολύ και 12 άτομα απάντησαν πάρα πολύ.

Τα ποσοστά των συχνοτήτων δείχνουν ότι: το 4,8% δεν θεωρεί καθόλου ότι η σωστή συμπεριφορά όσο αφορά τους κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι σημαντικές για την εταιρία του, επίσης ένα άλλο 4,8% τη θεωρεί λίγο σημαντική, το 14,3% δεν την θεωρεί ούτε λίγο ούτε πολύ σημαντική,το 19% τη θεωρεί πολύ σημαντική ενώ το 57,1% τη θεωρεί πάρα πολύ σημαντική.

Η μέση τιμή των δεδομένων είναι 4,19. Η τυπική απόκλιση είναι 1.167.Παρουσιάζεται και το αντίστοιχο ιστόγραμμα.

Κεφάλαιο πέμπτο

Συμπεράσματα

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η διερεύνηση των χρηματοοικονομικών επιπτώσεων των Κινδύνων του Κυβερνοχώρου στο χώρο εστίασης. Για το σκοπό αυτό, στο παρόν κείμενο έγινε προσπάθεια να παρουσιαστεί ο Γενικός Κανονισμός Προστασίας Δεδομένων, οι Κίνδυνοι του Κυβερνοχώρου αλλά και επιχειρηθούν να προσεγγιστούν οι επιπτώσεις των Κινδύνων στο χώρο εστίασης. Μέσα από την παρουσίαση των πιο σημαντικών εννοιών σχετικών με τα ανωτέρω θέματα, στο παρόν κεφάλαιο θα γίνει προσπάθεια παρουσίασης των βασικότερων συμπερασμάτων της παρούσας εργασίας.

Όσον αφορά το Γενικό Κανονισμό Προστασίας Δεδομένων, διαφαίνεται ότι, σε γενικές γραμμές, η επιστημονική κοινότητα συντάσσεται με την άποψη ότι πρόκειται περί ενός γόνιμου μέτρου και μιας προσπάθειας της Ευρωπαϊκής Ένωσης, προς την θετική κατεύθυνση, για την αποτελεσματικότερη και πιο αυστηρή προστασία της αξίας των προσωπικών δεδομένων των Ευρωπαίων χρηστών του διαδικτύου.

Σημαντικό είναι να αναφερθεί ότι ο Γενικός Κανονισμός Προστασίας δεδομένων είναι απόρροια της ραγδαίας ανάπτυξης της τεχνολογίας και των πολύπλοκων πληροφοριακών συστημάτων, που έχει οδηγήσει σε μια παράλληλη αύξηση, όχι μόνο των κρουσμάτων επιθέσεων στον παγκόσμιο κυβερνοχώρο, αλλά και της σοβαρότητας των κινδύνων αυτών, καθώς και των δυνητικών ευπαθειών των πληροφοριακών συστημάτων απέναντι στους κινδύνους αυτούς. Σύμφωνα μάλιστα με ορισμένες πρόσφατες εκτιμήσεις, το κόστος που συνεπάγονται οι κίνδυνοι του κυβερνοχώρου ανέρχεται έως και τα 600 δις. δολάρια, παγκοσμίως. Οι επιθέσεις αυτές προφανώς δεν αφήνουν ανεπηρέαστες τις επιχειρήσεις που δραστηριοποιούνται στο χώρο της εστίασης. Αξίζει βέβαια να σημειωθεί πως αυτό έχει τεράστιες οικονομικές επιπτώσεις για τις βιομηχανίες τροφίμων, γεγονός που διακυβεύει και τη λειτουργία αυτών.

Στο παρόν κεφάλαιο, σημαντικό είναι να αναφερθούν και τα σημαντικότερα συμπεράσματα από την έρευνα που πραγματοποιήθηκε και αφορά στις αντιλήψεις των επιχειρηματιών του ελληνικού κλάδου της εστίασης (κλάδος ποτών και τροφίμων) για την διασφάλιση των πληροφοριών από τους κινδύνους του κυβερνοχώρου. Ο

κύριος στόχος της συγκεκριμένης ποσοτικής έρευνας είναι να παρουσιάσει τα αποτελέσματα κάθε ερώτησης του ερωτηματολογίου σχετικά με τη συμπεριφορά των επιχειρηματιών, καθώς και τα περιγραφικά στατιστικά μέτρα που προκύπτουν από κάθε μία ερώτηση ξεχωριστά. Τα περιγραφικά μέτρα που θα εξεταστούν έχουν αριθμητική μορφή και αποτελούνται από στατιστικά στοιχεία, ποσοστά και άλλα μέτρα.

Στη πρώτη ερώτηση του ερωτηματολογίου που αφορά στη γνώση των δυνητικών κινδύνων, αναφορικά με την ασφάλεια των πληροφοριών, τα αποτελέσματα έδειξαν ότι ότι ο μέσος όρος των ατόμων που γνωρίζουν είναι ούτε λίγο ούτε πολύ, διότι προσεγγίζει την κατηγοριοποίηση 3. Επίσης, η τυπική απόκλιση είναι 1,195, όπου αντιπροσωπεύει το πόσο διεσπαρμένες είναι οι μεταβλητές από τον μέσο όρο.

Στη δεύτερη ερώτηση, που πραγματεύεται εάν οι επιχειρηματίες γνωρίζουν το κόστος παραβίασης της ασφάλειας πληροφοριών, το συμπέρασμα ήταν ο μέσος όρος των ατόμων δείχνει ότι έχουν λίγη γνώση. Ακολούθως, αναφορικά με την αντίληψη του κινδύνου διαρροής της ασφάλειας πληροφοριών, το αποτέλεσμα ήταν ότι ο μέσος όρος των ατόμων δείχνει ότι αντιλαμβάνονται πολύ τον κίνδυνο.

Εν συνεχεία, στη τέταρτη ερώτηση που αφορά στην ενημέρωση των επιχειρηματιών για την ενημέρωση τους αναφορικά με τη διαρροή πληροφοριών, το αποτέλεσμα ήταν ότι ο μέσος όρος των ατόμων ενημερώνεται λίγο και η τυπική απόκλιση της μέτρησης ήταν 1,426. Ακολούθως στο ερώτημα που αφορά στην επικοινωνία για το θέμα της ασφάλειας πληροφοριών για την ενίσχυση των γνώσεων των επιχειρηματιών, το αποτέλεσμα ήταν ότι ο μέσος όρος των ατόμων που συμμετείχαν στην έρευνα επικοινωνούν πολύ για θέματα ασφάλειας. Στη συνέχεια, στην ερώτηση που αφορούσε αν οι επιχειρηματίες στο χώρο εστίασης γνωρίζουν εάν οι κανονισμοί ασφαλείας και οι διαδικασίες που τις διέπουν είναι σημαντικές για την εταιρεία τους, το αποτέλεσμα ήταν ο μέσος όρος των ατόμων πιστεύει ότι είναι πολύ σημαντικοί οι κανονισμοί. Τώρα αν οι κανονισμοί αυτοί επηρεάζουν τη συμπεριφορά τους το αποτέλεσμα ήταν ότι ο μέσος όρος επηρεάζεται πολύ. Τέλος, η διερεύνηση της άποψης που αφορά στο αν η σωστή συμπεριφορά και η συμμόρφωση στους κανονισμούς ασφαλείας είναι σημαντικές για την εταιρεία, το συμπέρασμα ήταν ότι το 4,8% δεν θεωρεί καθόλου ότι η σωστή συμπεριφορά όσο αφορά τους κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι

σημαντικές για την εταιρία του, επίσης ένα άλλο 4,8% τη θεωρεί λίγο σημαντική, το 14,3% δεν την θεωρεί ούτε λίγο ούτε πολύ σημαντική,το 19% τη θεωρεί πολύ σημαντική ενώ το 57,1% τη θεωρεί πάρα πολύ σημαντική.

Συμπερασματικά, να αναφερθεί ότι σε γενικές γραμμές οι επιχειρηματίες στο χώρο της εστίασης αναγνωρίζουν τη σημαντικότητα των κανονισμών ασφαλείας για την επιχείρηση, ωστόσο δεν είναι βέβαιο κατά πόσο το ποσοστό αυτό εφαρμόζει τις πρακτικές αυτές στην επιχείρηση του ή κατά πόσο θεωρεί ότι αυτές είναι σημαντικές.

Κλείωντας το παρόν κείμενο, κρίνεται σημαντικό να αναφέρουμε ότι οι Κίνδυνοι του Κυβερνοχώρου ειδικότερα τα τελευταία χρόνια είναι αυξημένοι με σημαντικές επιπτώσεις, κυρίως οικνομικές για τις επιχειρήσεις. Για το λόγο αυτό κρίνεται σημαντικό οι εξελίξεις αυτές πρέπει να οδηγήσουν στην άνθιση του επαγγέλματος της ασφάλισης έναντι των κινδύνων αυτών. Για τις επιχειρήσεις, αυτό αποτελεί μια επιπρόσθετη επιλογή για τον σχεδιασμό του βέλτιστου προγράμματος διαχείρισης των εταιρικών κινδύνων, για τη διασφάλιση των πελατών αλλά για τη διασφάλιση της εύρυθμης λειτουργίας τους.

Βιβλιογραφία

Α. Ελληνική

1. Ελευθεριάδης, Ι. (2018). *Διοίκηση Εταιρικών Κινδύνων*. Πανεπιστημιακές Σημειώσεις.
2. Ιγγλεζάκης Ι. (2016). Η Συγκατάθεση στο Δίκαιο των προσωπικών δεδομένων, Νομική Βιβλιοθήκη, Αθήνα.
3. Κοτσαλής Λ. και Μενουδάκος Κ. (2018). Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και Πρακτική Εφαρμογή, 1η έκδοση, Νομική Βιβλιοθήκη, Αθήνα.
4. Καρατζά Λ. (2014). 4 Κώδικες, ΑΚ, ΚΠολΔ, ΠΚ, ΚΠΔ, ΣΥΝ 37, 40η έκδοση, Νομική Βιβλιοθήκη, Αθήνα.
5. Πατελάρου, Ε.& Μπροκαλάκη, Η.(2010). *Μεθοδολογία της Συστηματικής Ανασκόπησης και Μετα-ανάλυσης,* 49(2): 121-122. Διαθέσιμο: http://www.hjn.gr/actions/get_pdf.php?id=218.

Β. Ξενόγλωσση

1. Böhme, R. and Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", Workshop on Economics of Information Security (WEIS), [online], Διαθέσιμο στο: https://www.econinfosec.org/archive/weis2006/docs/16.pdf .
2. De Hert, P. and Papakonstantinou, V. (2016), "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review*, 32 (2), pp. 179-194.
3. Eling, M. and Wirfs, J., H, (2016), "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", Institute of Insurance Economics, [online], Διαθέσιμο στο: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf .
4. Mukhopadhyay, A., Saha, D., Chakrabarti, B., B., Mahanti, A. and Podder, A. (2005), "Insurance for Cyber-risk: A Utility Model", *Decision*, 32 (1), pp. 1-19.
5. Ögüt, H., Raghunathan, S., and 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*, 31 (3), pp. 497–512.

6. Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", *Network Security*, 17 (6), pp. 8-11.

Παράρτημα Α: Ερωτηματολόγιο

Απαντήστε στο παρακάτω ερωτηματολόγιο που ααφορά στη διασφάλιση πληροφοριών της εταιρίας σας από το 1 εως το 5.

1. ΚΑΘΟΛΟΥ 5.ΠΑΡΑ ΠΟΛΎ

	1	2	3	4	5
Γνωρίζω για δυνητικούς κινδύνους όσο αφορά στην ασφάλεια πληροφοριών					
Έχω αρκετή γνώση όσο αφορά το κόστος παραβίασης ασφάλειας πληροφοριών					
Αντιλαμβάνομαι τον κίνδυνο της διαρροής ασφάλειας πληροφοριών					
Ενημερώνομαι όσο αφορά στην ασφάλεια πληροφοριών					
Μοιράζομαι όσα ξέρω για την ασφάλεια πληροφοριών για να ενισχύσω τη γνώση μου					
Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν είναι σημαντικοι για την εταιρία μου					
Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν επηρεάζουν τη συμπεριφορά μου					
Οι κανονισμοί ασφάλειας πληροφοριών και οι διαδικασίες που τους διέπουν, έχουν εφιστήσει την προσοχή μου					
Η σωστή συμπεριφορά όσο αφορά τους κανονισμούς ασφάλειας πληροφοριών καθώς και των διαδικασιών που τους διέπουν είναι σημαντικές για την εταιρία μου					