ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΜΣ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

Προστασία Προσωπικών Δεδομένων στις Επιχειρήσεις

Σπυρίδη Αικατερίνη

Α.Μ. : 41kA/2022

Επιβλέπων : Δημήτριος Αηδόνης Καθηγητής

Φεβρουάριος, 2024

Περίληψη

Η παρούσα μελέτη εστιάζει στον σημαντικό ρόλο της προστασίας προσωπικών δεδομένων στο πλαίσιο των επιχειρήσεων. Στην εργασία αυτή, εξετάζεται η σημασία της προστασίας της ιδιωτικότητας των πελατών και των συνεργατών και η επίδρασή της στις επιχειρησιακές δραστηριότητες, τους κινδύνους και τις προκλήσεις που σχετίζονται με τη διαχείριση και την προστασία των προσωπικών δεδομένων σε διάφορους τομείς της επιχειρηματικής δραστηριότητας.

Η αιτιολόγηση της σπουδαιότητας του θέματος βασίζεται στην αυξανόμενη χρήση δεδομένων και την επιβολή νομοθεσίας όπως το GDPR. Είναι σημαντικό, λοιπόν, να εξεταστούν η σημασία, οι κίνδυνοι και οι τρόποι αντιμετώπισης των προκλήσεων που σχετίζονται με την προστασία των δεδομένων και η επίδρασή της στο επιχειρηματικό περιβάλλον.

Η μελέτη αναλύει τον ρόλο της προστασίας προσωπικών δεδομένων στις επιχειρήσεις και επισημαίνει τη σημασία της διατήρησης της ιδιωτικότητας των πελατών και των συνεργατών. Επιπλέον, εξετάζονται οι επιπτώσεις των παραβιάσεων δεδομένων στις επιχειρήσεις, καθώς και η σχέση ανάμεσα στην προστασία δεδομένων και την εμπιστοσύνη των πελατών και τη φήμη της επιχείρησης. Στη συνέχεια, αναφέρονται οι κύριοι κίνδυνοι παραβίασης δεδομένων και οι προκλήσεις που προκύπτουν στη διαχείριση και προστασία των προσωπικών δεδομένων. Επιπλέον, παρουσιάζονται στρατηγικές για την προστασία των δεδομένων και πρακτικά παραδείγματα προστασίας. Το επόμενο κεφάλαιο εξετάζει τα νομικά θέματα και τη συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR). Αναλύονται οι νομικές απαιτήσεις και οι προκλήσεις που προκύπτουν στη συμμόρφωση με τον κανονισμό. Στη συνέχεια, παρουσιάζεται η μεθοδολογία της έρευνας, συμπεριλαμβανομένης της συλλογής και ανάλυσης δεδομένων. Αναφέρονται επίσης τα αποτελέσματα ανάλυσης δεδομένων και η συζήτησή τους. Στο τέλος της μελέτης, παρουσιάζονται τα συμπεράσματα της μελέτης και η σημασία της προστασίας δεδομένων στις επιχειρήσεις. Επίσης, περιλαμβάνεται η βιβλιογραφία και ένα παράρτημα με περαιτέρω πληροφορίες.

Η έρευνα διαπιστώνει ότι η επίγνωση των επιχειρηματιών για τη σημασία της προστασίας δεδομένων είναι σημαντική, αλλά υπάρχουν προκλήσεις στην εφαρμογή της νομοθεσίας. Τα αποτελέσματα δείχνουν μέτριο βαθμό συμμόρφωσης με το GDPR και τη σημασία της εκπαίδευσης των εργαζομένων σε θέματα προστασίας δεδομένων. Παράλληλα,

υπογραμμίζεται η ανάγκη σεβασμού του διαδικτυακού απορρήτου και της ιδιωτικότητας των ατόμων. Επιπρόσθετα η έρευνα αναδεικνύει τη σημασία της προστασίας δεδομένων στις επιχειρήσεις και τονίζει την ανάγκη για συμμόρφωση με τη νομοθεσία και την εφαρμογή αρχών προστασίας προσωπικών δεδομένων.

Λέξεις- κλειδιά: Προστασία Προσωπικών Δεδομένων, GDPR, Επιχειρήσεις, Ιδιωτικότητα, Νομική Συμμόρφωση

Abstract

This study focuses on the significant role of personal data protection in the context of businesses. In this work, the importance of safeguarding the privacy of customers and partners is examined, along with its impact on business activities, risks, and challenges related to the management and protection of personal data in various business sectors.

The justification for the importance of this topic is based on the increasing use of data and the enforcement of legislation such as GDPR. Therefore, it is crucial to explore the significance, risks, and methods of addressing the challenges associated with data protection and its impact on the business environment.

The study analyzes the role of personal data protection in businesses and underscores the importance of maintaining the privacy of customers and partners. Furthermore, it examines the consequences of data breaches on businesses, as well as the relationship between data protection and customer trust and the reputation of the business.

The study also highlights the main risks of data breaches and the challenges that arise in the management and protection of personal data. Additionally, it presents strategies for data protection and practical examples of protection measures. The following chapter discusses legal issues and compliance with the General Data Protection Regulation (GDPR), including legal requirements and challenges associated with compliance.

Furthermore, the methodology of the research is presented, including data collection and analysis. The results of data analysis and their discussion are also provided. In conclusion, the study emphasizes the importance of data protection in businesses and the need for compliance with legislation and the implementation of data protection principles.

Keywords: Personal Data Protection, GDPR, Businesses, Privacy, Legal Compliance

Περιεχόμενα

Εισαγωγή 9

Κεφάλαιο 1ο: Προστασία Προσωπικών Δεδομένων: Θεωρητική Προσέγγιση 12

1.1 Ορισμός και σημασία της προστασίας προσωπικών δεδομένων 12

1.2 Νομοθετικό Πλαίσιο: Ανασκόπηση του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) και Άλλων Σχετικών Νομοθεσιών 13

1.3 Αρχές προστασίας προσωπικών δεδομένων 15

Κεφάλαιο 2ο: Σημασία της Προστασίας των Δεδομένων στις Επιχειρήσεις 19

2.1 Επιπτώσεις των παραβιάσεων δεδομένων 20

2.2 Επίδραση στην εμπιστοσύνη των πελατών 22

2.3 Σχέση με την επιχειρηματική επίδοση και τη φήμη 23

Κεφάλαιο 3ο: Κίνδυνοι και Προκλήσεις Προστασίας των Δεδομένων στις Επιχειρήσεις 25

3.1 Κύριοι κίνδυνοι παραβίασης δεδομένων 26

3.2 Προκλήσεις στη Διαχείριση και Προστασία των Προσωπικών Δεδομένων 27

Κεφάλαιο 4ο: Εφαρμογή της Προστασίας Δεδομένων στις Επιχειρήσεις 30

4.1 Στρατηγικές για την προστασία των προσωπικών δεδομένων 30

4.1.1 Εφαρμογή Στρατηγικών Προστασίας Δεδομένων 30

4.1.2 Βασικές Εκτιμήσεις Κατά την Εφαρμογή Στρατηγικών Προστασίας Δεδομένων 30

4.2 Εφαρμογή των αρχών της προστασίας δεδομένων στις επιχειρήσεις 31

4.2.1 Βασικές Αρχές Προστασίας Δεδομένων που Θα Πρέπει να Εφαρμόζονται από τις Επιχειρήσεις 31

4.2.2 Εφαρμογή των Αρχών Προστασίας Δεδομένων στην Πράξη από τις Επιχειρήσεις 32

4.3 Παραδείγματα πρακτικών προστασίας 33

Κεφάλαιο 5ο: Νομικά Θέματα και Συμμόρφωση 35

5.1 Ανάλυση των νομικών πτυχών σχετικά με την προστασία των δεδομένων 35

5.2 Προκλήσεις στη συμμόρφωση με το GDPR και άλλους κανονισμούς 38

Κεφάλαιο 6ο: Μεθοδολογία 43

6.1 Σκοπός και ερευνητικά ερωτήματα 43

6.2 Δείγμα 43

6.3 Μέθοδος συλλογής δεδομένων 43
6.4 Διαδικασία 45
6.5 Στατιστική ανάλυση 45
Κεφάλαιο 7^{ο}: Αποτελέσματα 47
7.1 Περιγραφική στατιστική 47
7.2 Επαγωγική στατιστική 62
Κεφάλαιο 8^{ο}: Συζήτηση 75
Συμπεράσματα 80
Βιβλιογραφία 82
Παράρτημα 94

Κατάλογος περιεχομένων Πινάκων

Πίνακας 1. Μέση τιμή και τυπική απόκλιση της γνώσης για το Γενικό Κανονισμό για την Προστασία των Δεδομένων 52

Πίνακας 2. Μέσες τιμές και τυπικές αποκλίσεις για τις αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων 62

Πίνακας 3. Mann-Whitney tests για διερεύνηση διαφοροποιήσεων ανάλογα το φύλο 66

Πίνακας 4. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα την ηλικία 66

Πίνακας 5. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το μορφωτικό επίπεδο 67

Πίνακας 6. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα τη θέση στην επιχείρηση 68

Πίνακας 7. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το είδος της επιχείρησης 68

Πίνακας 8. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το μέγεθος της επιχείρησης 69

Πίνακας 9. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα τον τομέα δραστηριοποίησης της επιχείρησης 70

Πίνακας 10. Chi-square tests για τη διερεύνηση διαφοροποιήσεων ανάλογα τα δημογραφικά χαρακτηριστικά 72

Κατάλογος περιεχομένων διαγραμμάτων

Διάγραμμα 1. Φύλο 47

Διάγραμμα 2. Ηλικία 48

Διάγραμμα 3. Μορφωτικό επίπεδο 48

Διάγραμμα 4. Θέση στην επιχείρηση 49

Διάγραμμα 5. Είδος επιχείρησης 50

Διάγραμμα 6. Μέγεθος επιχείρησης 50

Διάγραμμα 7. Τομέας δραστηριοποίησης επιχείρησης 51

Διάγραμμα 8. Γνώση του Γενικού Κανονισμού για την Προστασία των Δεδομένων 51

Διάγραμμα 9. Εκπαίδευση εργαζομένων σε θέματα που αφορούν το Γενικό Κανονισμό για την Προστασία των Δεδομένων 52

Διάγραμμα 10. Διατήρηση προσωπικών δεδομένων 53

Διάγραμμα 11. Διαμοιρασμός προσωπικών δεδομένων 53

Διάγραμμα 12. Χρήση προσωπικών δεδομένων για προωθητικές ενέργειες πωλήσεων 54

Διάγραμμα 13. Κατανοητός και απλός τρόπος της δυνατότητας διαγραφής 54

Διάγραμμα 14. Γνώση φυσικών προσώπων για κατοχή και χρήση των προσωπικών δεδομένων τους 55

Διάγραμμα 15. Χρονική διάρκεια διατήρησης προσωπικών δεδομένων 56

Διάγραμμα 16. Ακρίβεια και ενημέρωση προσωπικών δεδομένων 56

Διάγραμμα 17. Ασφαλής διατήρηση των προσωπικών δεδομένων 57

Διάγραμμα 18. Γνώση των δικαιωμάτων των ατόμων των οποίων διατηρούνται και αποθηκεύονται τα προσωπικά τους δεδομένα 58

Διάγραμμα 19. Δικαιώματα που μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα 58

Διάγραμμα 20. Λεπτομερής περιγραφή της πολιτικής απορρήτου προσωπικών δεδομένων στην ιστοσελίδα της επιχείρησης 59

Διάγραμμα 21. Ευκολία προσαρμογής στο Γενικό Κανονισμό για την Προστασία των Δεδομένων 60

Διάγραμμα 22. Δυσκολία εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων 60

Διάγραμμα 23. Κόστος εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων 61

Διάγραμμα 24. Μείωση εσόδων της επιχείρησης εξαιτίας του Γενικού Κανονισμού για την Προστασία των Δεδομένων 61

Εισαγωγή

Στην εποχή της ψηφιακής τεχνολογίας και της εκρηκτικής αύξησης των δεδομένων, η προστασία της προσωπικής πληροφορίας και η διασφάλιση της ιδιωτικότητας αποτελούν κεντρικούς πυλώνες στην ανάπτυξη και τη λειτουργία των σύγχρονων οργανισμών. Η ανάγκη για συμμόρφωση με τους διεθνείς κανονισμούς προστασίας δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, επιβάλλει νέες προκλήσεις και απαιτήσεις για τους οργανισμούς, απαιτώντας από αυτούς να ενσωματώσουν αυστηρά πρωτόκολλα και διαδικασίες για την προστασία των δεδομένων. Η διαχείριση και η προστασία των προσωπικών δεδομένων δεν αποτελεί μόνο νομική υποχρέωση, αλλά επιβάλλεται και ως ηθική επιταγή, αναδεικνύοντας την ανάγκη για συνεχή ενημέρωση, προσαρμογή και βελτίωση των εσωτερικών μηχανισμών ασφάλειας και προστασίας δεδομένων.

Παράλληλα, οι συνεχείς τεχνολογικές εξελίξεις και η αλλαγή του ψηφιακού τοπίου προσθέτουν επιπλέον πολυπλοκότητα στην εφαρμογή και την τήρηση των κανονισμών. Η ανάλυση των προκλήσεων, των βέλτιστων πρακτικών και των στρατηγικών για την αποτελεσματική συμμόρφωση με τους κανονισμούς προστασίας δεδομένων αποτελεί ζωτικής σημασίας στοιχείο για τη διασφάλιση της ιδιωτικότητας, της εμπιστοσύνης και της ασφάλειας των προσωπικών δεδομένων σε μια παγκοσμιοποιημένη και ψηφιακά διασυνδεδεμένη κοινωνία.

Στον πυρήνα της σύγχρονης επιχειρηματικής στρατηγικής βρίσκεται η κατανόηση της αξίας των προσωπικών δεδομένων, όχι μόνο ως πηγής επιχειρηματικής πληροφόρησης αλλά και ως πεδίο ευθυνών και ηθικών υποχρεώσεων. Η διαρκής εξέλιξη της τεχνολογίας και η επέκταση των ψηφιακών δικτύων έχουν πολλαπλασιάσει τις ευκαιρίες για τη συλλογή, ανάλυση και χρήση προσωπικών δεδομένων, αναδεικνύοντας ταυτόχρονα νέες προκλήσεις για την προστασία της ιδιωτικότητας των πελατών και των συνεργατών.

Η σημασία της προστασίας των προσωπικών δεδομένων στο επιχειρηματικό περιβάλλον είναι πολυεπίπεδη. Αφενός, συμβάλλει στην κατασκευή ενός ισχυρού ηθικού πλαισίου και της εμπιστοσύνης μεταξύ των επιχειρήσεων και των πελατών τους, ενισχύοντας την εταιρική φήμη και την πελατειακή αφοσίωση. Αφετέρου, η αποτελεσματική διαχείριση και προστασία των προσωπικών δεδομένων αποτρέπει νομικές παραβάσεις και τις συνακόλουθες

οικονομικές ή φήμης κυρώσεις που μπορεί να προκύψουν από τη μη συμμόρφωση με τη νομοθεσία.

Η επιλογή του ερευνητικού αντικειμένου αυτού είναι σπουδαία καθώς αντικατοπτρίζει την αναγκαιότητα για ένα ισορροπημένο πλαίσιο στην επιχειρηματική χρήση των δεδομένων. Η αιτιολόγηση της σπουδαιότητας του θέματος αυτού βασίζεται σε πολλούς λόγους.

Καταρχάς, η αύξηση της ψηφιακής επικοινωνίας και της διαδικτυακής παρουσίας επιχειρήσεων σημαίνει ότι συλλέγονται, αποθηκεύονται και επεξεργάζονται περισσότερα προσωπικά δεδομένα από ποτέ προηγουμένως. Αυτό αυξάνει τον κίνδυνο για παραβάσεις ασφαλείας και προκλήσεις στη διαχείριση των δεδομένων.

Δεύτερον, η θέσπιση νομοθεσίας όπως το Γενικό Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης έχει θέσει πρότυπα για την προστασία των προσωπικών δεδομένων που αφορούν τους πολίτες και τους πελάτες. Αν οι επιχειρήσεις δεν συμμορφώνονται με αυτήν τη νομοθεσία, μπορούν να αντιμετωπίσουν σημαντικές κυρώσεις.

Τέλος, η επίδραση της προστασίας προσωπικών δεδομένων στην επιχειρηματική δραστηριότητα είναι σημαντική. Από τη διαχείριση της πληροφορίας πελατών και συνεργατών μέχρι τη δημιουργία ασφαλών ψηφιακών υποδομών, η προστασία των προσωπικών δεδομένων έχει ευρύ φάσμα επιδράσεων στην επιχειρηματική διαδικασία.

Συνοψίζοντας, η προστασία των προσωπικών δεδομένων στο πλαίσιο των επιχειρήσεων είναι ένα θέμα κρίσιμης σημασίας που απαιτεί την προσοχή και τη συμμόρφωση των επιχειρήσεων με τη νομοθεσία και τις καλές πρακτικές προκειμένου να διασφαλίσουν την ιδιωτικότητα των πελατών και των συνεργατών τους και να ανταποκριθούν στις απαιτήσεις της σύγχρονης επιχειρηματικής πραγματικότητας.

Η παρούσα μελέτη επιδιώκει να εμβαθύνει στην κατανόηση του ζωτικού ρόλου της προστασίας προσωπικών δεδομένων στον επιχειρηματικό κόσμο, καθώς και της σημασίας της διασφάλισης της ιδιωτικότητας των πελατών και των συνεργατών. Πιο συγκεκριμένα, ο σκοπός της είναι να διερευνήσει την επίδραση της προστασίας δεδομένων στις επιχειρηματικές διαδικασίες, τους κινδύνους και τις προκλήσεις που συνδέονται με τη διαχείριση των προσωπικών δεδομένων, καθώς και τις στρατηγικές προστασίας και συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR).

Οι στόχοι της μελέτης περιλαμβάνουν:

- Την κατανόηση της σημασίας της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας στο επιχειρηματικό περιβάλλον.
- Την ανάλυση των επιπτώσεων παραβιάσεων δεδομένων στις επιχειρήσεις και την εμπιστοσύνη των πελατών.
- Την εξέταση των κινδύνων και των προκλήσεων που εγείρονται από τη διαχείριση προσωπικών δεδομένων και την ανάπτυξη στρατηγικών προστασίας.
- Την ανάλυση των νομικών πτυχών και των προκλήσεων στη συμμόρφωση με το GDPR και άλλες σχετικές νομοθεσίες.
- Την παρουσίαση πρακτικών παραδειγμάτων και στρατηγικών που εφαρμόζονται από επιχειρήσεις για την προστασία των δεδομένων.

Αρχικά αναλύεται ο ορισμός και η σημασία της προστασίας δεδομένων, παρέχοντας παράλληλα μια σαφή εικόνα του νομοθετικού πλαισίου που διέπει τον τομέα αυτόν, με ιδιαίτερη έμφαση στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).

Επιπρόσθετα, εξετάζεται η επιρροή της προστασίας δεδομένων στην εμπιστοσύνη των πελατών και στην επιχειρηματική φήμη, καθώς και οι επιπτώσεις των παραβιάσεων δεδομένων στις επιχειρήσεις. Αναδεικνύονται οι κίνδυνοι και οι προκλήσεις που ανακύπτουν από τη διαχείριση προσωπικών δεδομένων, παρουσιάζοντας παράλληλα στρατηγικές και πρακτικά παραδείγματα για την αποτελεσματική προστασία δεδομένων.

Η μελέτη διερευνά επίσης μέσω ποσοτικής έρευνας τις νομικές πτυχές και τις προκλήσεις στη συμμόρφωση με το GDPR, αναλύοντας τις νομικές απαιτήσεις και τις εφαρμοζόμενες πρακτικές στον τομέα της προστασίας δεδομένων. Η μελέτη καταλήγει με την παρουσίαση των αποτελεσμάτων, τη συζήτηση των ευρημάτων και την προσφορά συμπερασμάτων που ενισχύουν την κατανόηση της σημασίας της προστασίας προσωπικών δεδομένων στην επιχειρηματική στρατηγική και λειτουργία. Συνοψίζει τα κυριότερα ευρήματα και παρέχει συστάσεις για τη βελτίωση των πρακτικών προστασίας δεδομένων, καθώς και προτάσεις για μελλοντικές έρευνες.

Κεφάλαιο 1ο: Προστασία Προσωπικών Δεδομένων: Θεωρητική Προσέγγιση

1.1 Ορισμός και σημασία της προστασίας προσωπικών δεδομένων

Η προστασία προσωπικών δεδομένων αποτελεί έναν τομέα ουσιαστικής σημασίας στη σύγχρονη εποχή, καθώς η διασφάλιση της ασφάλειας, της αξιοπιστίας και της ιδιωτικότητας των δεδομένων αναδεικνύεται σε κρίσιμη προτεραιότητα. Η πρόκληση εντείνεται με την εμφάνιση των πλατφορμών cloud, που προσθέτουν ένα επιπλέον επίπεδο πολυπλοκότητας στο οικοσύστημα των δεδομένων, εισάγοντας κινδύνους που απειλούν την ακεραιότητα των δεδομένων. Η προστασία προσωπικών δεδομένων καθίσταται αναγκαία για την αποτροπή εκμετάλλευσης των συστημάτων cloud από κακόβουλους παράγοντες (Bertino, 2016).

Η πολυπλοκότητα της κοινής χρήσης δεδομένων αυξάνεται λόγω της διαθεσιμότητας πολλαπλών συνόλων δεδομένων, ενώ η διάχυτη συλλογή δεδομένων από πλήθος συσκευών επιδεινώνει το πρόβλημα ασφαλείας και απορρήτου. Αντιμετωπίζοντας αυτές τις προκλήσεις, η εκτεταμένη έρευνα στην αξιοπιστία δεδομένων αποτελεί προϋπόθεση για την ανάπτυξη αποτελεσματικών τεχνικών, ενώ οι τεχνικές αξιολόγησης αξιοπιστίας και οι προσεγγίσεις συγχώνευσης ετερογενών πολιτικών ελέγχου πρόσβασης είναι καθοριστικής σημασίας για τη διασφάλιση της ακεραιότητας των δεδομένων (Bertino, 2016).

Η σημασία της προστασίας προσωπικών δεδομένων είναι πολυεπίπεδη και συνδέεται άμεσα με τη διασφάλιση των ατομικών δικαιωμάτων, όπως η ιδιωτικότητα και η πληροφοριακή αυτοδιάθεση. Η ανάλυση μεγάλων δεδομένων και η επεξεργασία δεδομένων μπορεί να οδηγήσει σε μεροληπτικές και επεμβατικές μορφές επεξεργασίας, ενώ η προστασία των προσωπικών δεδομένων αποτελεί ουσιαστικό μέσο για την πρόληψη των πιθανών βλαβών από τέτοιες πρακτικές. Παράλληλα, η συλλογική διάσταση της προστασίας δεδομένων υπογραμμίζει την ανάγκη για προστασία ομάδων προσώπων και απαιτείται περισσότερο ολοκληρωμένα μέτρα προστασίας για την αντιμετώπιση των κινδύνων και των ζητημάτων που ενδέχεται να προκύψουν (Mantelero, 2016).

Όσον αφορά τους πιθανούς κινδύνους από παραβιάσεις δεδομένων, αυτοί είναι σημαντικοί και πολυδιάστατοι. Οι παραβιάσεις μπορεί να οδηγήσουν σε κλοπή ταυτότητας, απάτες κοινωνικής μηχανικής, οικονομική ζημιά και ζημιά στη φήμη, ενώ η μη ειδοποίηση των

υποκειμένων των δεδομένων για παραβιάσεις μπορεί να οδηγήσει σε βλάβη των δικαιωμάτων και των ελευθεριών τους (Nieuwesteeg & Faure, 2018).

Η νομοθεσία της Ευρωπαϊκής Ένωσης (ΕΕ) απαιτεί την κοινοποίηση και την καταγραφή περιστατικών που προκαλούν πραγματική δυσμενή επίδραση στα προσωπικά δεδομένα, υποχρεώνοντας τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να κατανοήσουν τη διαφορά μεταξύ παραβίασης προσωπικών δεδομένων και παραβίασης ασφάλειας, ώστε να συμμορφώνονται με τις απαιτήσεις κοινοποίησης παραβίασης (Nieuwesteeg & Faure, 2018).

Οι οργανισμοί πρέπει να υιοθετούν προληπτικά μέτρα για τον μετριασμό των κινδύνων που σχετίζονται με παραβιάσεις δεδομένων, συμπεριλαμβανομένης της εφαρμογής ισχυρών μέτρων ασφαλείας, της διενέργειας τακτικών ελέγχων ασφαλείας και της διασφάλισης της συμμόρφωσης με τους σχετικούς νόμους και κανονισμούς (Nieuwesteeg & Faure, 2018).

Συνοψίζοντας, η προστασία προσωπικών δεδομένων αποτελεί ένα θέμα ζωτικής σημασίας στην εποχή των μεγάλων δεδομένων και της εξάπλωσης των τεχνολογιών cloud computing. Η ανάγκη για ενισχυμένη ασφάλεια, αξιοπιστία δεδομένων, και προστασία της ιδιωτικότητας καθίσταται προφανής μέσα από την εξέταση των προκλήσεων και των κινδύνων που παρουσιάζονται. Η συμμόρφωση με τις νομοθεσίες και η εφαρμογή προηγμένων τεχνολογικών λύσεων είναι καθοριστικής σημασίας για την επίτευξη ενός ασφαλέστερου περιβάλλοντος δεδομένων, προστατεύοντας έτσι τα άτομα και τις οργανώσεις από τις δυσμενείς συνέπειες των παραβιάσεων δεδομένων.

1.2 Νομοθετικό Πλαίσιο: Ανασκόπηση του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) και Άλλων Σχετικών Νομοθεσιών

Η νομοθεσία που διέπει την προστασία των προσωπικών δεδομένων περιλαμβάνει διάφορους νόμους και κανονισμούς σε παγκόσμιο επίπεδο. Στο επίκεντρο της ευρωπαϊκής νομοθεσίας βρίσκεται ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR), ο οποίος αποτελεί την πιο σημαντική νομοθετική πρωτοβουλία για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση (ΕΕ) (Dove, 2018). Ο

GDPR, ο οποίος θέτει το πλαίσιο για την επεξεργασία προσωπικών δεδομένων, αντικατέστησε την προηγούμενη οδηγία 95/46/ΕΚ, ενισχύοντας τις εγγυήσεις και την προστασία των δικαιωμάτων των ατόμων (Dove, 2018).

Εκτός από τον GDPR, διάφορες χώρες έχουν εισάγει τους δικούς τους νόμους και κανονισμούς για την προστασία δεδομένων, ενισχύοντας τις πολιτικές προστασίας δεδομένων σε εθνικό επίπεδο (Olukoya, 2022). Οργανισμοί και επιχειρήσεις που διαχειρίζονται προσωπικά δεδομένα καλούνται να συμμορφωθούν με τις απαιτήσεις αυτών των νομοθεσιών, εφαρμόζοντας τις απαραίτητες πολιτικές ασφάλειας και απορρήτου (Olukoya, 2022). Ενδεικτικά, ο νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (Health Insurance Portability and Accountability Act - HIPAA) στις Ηνωμένες Πολιτείες αποτελεί έναν από τους κανονισμούς που αφορούν την προστασία των προσωπικών δεδομένων σε άλλη νομοθετική δικαιοδοσία (Olukoya, 2022).

Ο GDPR εισάγει σημαντικές απαιτήσεις και εγγυήσεις, όπως την υποχρέωση διορισμού εκπροσώπου στην ΕΕ για τους υπευθύνους επεξεργασίας δεδομένων, εκτός από περιπτώσεις που αφορούν δημόσιες αρχές ή φορείς (Dove, 2018). Περαιτέρω, ο κανονισμός προβλέπει την υποχρέωση ενημέρωσης για παραβιάσεις προσωπικών δεδομένων, ενισχύοντας τη διαφάνεια και την προστασία των δικαιωμάτων των ατόμων.

Εκτός από τον GDPR, πρόσθετες σχετικές νομοθεσίες περιλαμβάνουν πολιτειακούς νόμους στις Ηνωμένες Πολιτείες όπως ο Νόμος περί Ασφάλειας Πληροφοριών, καθώς και πρόσφατες ευρωπαϊκές πρωτοβουλίες όπως ο Νόμος για τις Ψηφιακές Υπηρεσίες και ο Νόμος για τις Ψηφιακές Αγορές, οι οποίοι επιδιώκουν να ενισχύσουν την προστασία δεδομένων και τη διαφάνεια στον ψηφιακό χώρο (Mizarhi-Borohovich et al., 2024).

Η συνεχής εξέλιξη του νομοθετικού πλαισίου απαιτεί από τους οργανισμούς να παραμένουν ενημερωμένοι και να προσαρμόζονται στις νέες απαιτήσεις για να διασφαλίζεται η συμμόρφωση και η αποτελεσματική προστασία των προσωπικών δεδομένων. Συνοψίζοντας, η συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) και άλλες σχετικές νομοθεσίες αποτελεί κρίσιμο στοιχείο για την ενίσχυση της προστασίας των προσωπικών δεδομένων σε ένα παγκοσμιοποιημένο περιβάλλον. Οι οργανισμοί οφείλουν να λαμβάνουν υπόψη τις διάφορες νομοθετικές απαιτήσεις και να εφαρμόζουν τις απαραίτητες πολιτικές και διαδικασίες για τη διασφάλιση της επαρκούς προστασίας των δεδομένων που διαχειρίζονται. Η συνεχής αναθεώρηση και ενημέρωση των μέτρων ασφαλείας και προστασίας δεδομένων είναι απαραίτητη για την

αντιμετώπιση των εξελισσόμενων απειλών και την προσαρμογή στις νέες νομοθετικές εξελίξεις. Επιπλέον, η διεθνής συνεργασία και ο συντονισμός μεταξύ των κρατών μελών και άλλων διεθνών εταίρων είναι ουσιαστικοί για την επίτευξη μιας αποτελεσματικής προστασίας δεδομένων σε παγκόσμιο επίπεδο.

1.3 Αρχές προστασίας προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων στηρίζεται σε μια σειρά από θεμελιώδεις αρχές, οι οποίες είναι ουσιώδεις για τη διασφάλιση της ιδιωτικότητας των ατόμων. Οι αρχές αυτές, όπως αναλύονται από τον Bygrave (2010), περιλαμβάνουν τη δίκαιη και νόμιμη επεξεργασία, την ελαχιστοποίηση των δεδομένων, την προδιαγραφή σκοπού, την ποιότητα των πληροφοριών, τη συμμετοχή και τον έλεγχο από το υποκείμενο των δεδομένων, τον περιορισμό της αποκάλυψης, την ασφάλεια των πληροφοριών και την ευαισθησία. Επιπλέον, τονίζεται ότι υπάρχει σημαντική επικάλυψη μεταξύ αυτών των κατηγοριών.

Η θεμελιώδης αρχή της προστασίας προσωπικών δεδομένων είναι η απαίτηση ότι τα δεδομένα δεν πρέπει να επεξεργάζονται χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων. Η ευαισθησία των προσωπικών δεδομένων διαμορφώνεται από το πλαίσιο στο οποίο χρησιμοποιούνται τα δεδομένα. Η ευρωπαϊκή οδηγία και η συνακόλουθη νομοθεσία στα κράτη μέλη επιτρέπουν στα άτομα να έχουν πρόσβαση όχι μόνο στα δικά τους δεδομένα αλλά και σε πληροφορίες σχετικά με το πώς χρησιμοποιούνται αυτά τα δεδομένα. Η αρχή της ελαχιστοποίησης των δεδομένων και η περιορισμένη αποκάλυψη υπογραμμίζουν την ανάγκη για συγκράτηση κατά τη συλλογή και χρήση προσωπικών δεδομένων.

- Σκοπός Κάθε Αρχής

Ο σκοπός των αρχών προστασίας προσωπικών δεδομένων ενσωματώνει την παροχή ενός πλαισίου για την ενδεδειγμένη επεξεργασία, χρήση και διαχείριση των προσωπικών δεδομένων. Αυτές οι αρχές υποστηρίζουν τη διαφάνεια, τη λογοδοσία και την ενδυνάμωση των ατόμων σε σχέση με τα δεδομένα τους, ενώ ταυτόχρονα περιορίζουν τις επιπτώσεις στην ιδιωτική ζωή και προστατεύουν εναντίον της καταχρηστικής χρήσης των δεδομένων.

- Εφαρμογή στην Πράξη

Η εφαρμογή των αρχών προστασίας προσωπικών δεδομένων απαιτεί από τους οργανισμούς να υιοθετούν μια συνεπή και ολοκληρωμένη προσέγγιση. Η χρήση τεχνολογιών ενίσχυσης

της ιδιωτικότητας (PETs) και η ανάπτυξη ενός πλαισίου διακυβέρνησης δεδομένων είναι κρίσιμα στοιχεία για την επίτευξη συμμόρφωσης. Επιπλέον, η διαρκής εκπαίδευση και ευαισθητοποίηση, καθώς και η εφαρμογή πολιτικών και διαδικασιών προστασίας δεδομένων, ενισχύουν την προστασία των προσωπικών δεδομένων.

- Συμμόρφωση με το Νομοθετικό Πλαίσιο

Για τη διασφάλιση της συμμόρφωσης με το νομοθετικό πλαίσιο, οι οργανισμοί πρέπει να υιοθετήσουν πρακτικές που ενσωματώνουν την αξιολόγηση κινδύνου και τη διαχείριση δεδομένων στις καθημερινές τους λειτουργίες. Ο διορισμός ενός Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO) και η εφαρμογή μιας πολιτικής προστασίας δεδομένων που περιλαμβάνει τις αρχές της ελάχιστης απαραίτητης επεξεργασίας, της διαφάνειας και της ασφάλειας είναι βασικά στοιχεία για την επίτευξη αυτού του στόχου. Η συνεχής επιθεώρηση και αξιολόγηση των μέτρων ασφαλείας, καθώς και η ενημέρωση των πολιτικών και διαδικασιών σύμφωνα με τις τελευταίες νομοθετικές αλλαγές, είναι επίσης απαραίτητες για τη διατήρηση της συμμόρφωσης.

Οι οργανισμοί πρέπει να διασφαλίζουν ότι όλοι οι εργαζόμενοι και οι συνεργάτες είναι ενημερωμένοι για τις απαιτήσεις προστασίας δεδομένων και να προωθούν μια κουλτούρα απορρήτου εντός της οργάνωσης. Η εκπαίδευση και η ευαισθητοποίηση του προσωπικού σχετικά με τις πρακτικές προστασίας δεδομένων και τις σχετικές νομοθετικές απαιτήσεις είναι ζωτικής σημασίας.

- Πιθανές Συνέπειες της Μη Συμμόρφωσης

Η μη συμμόρφωση με τους νόμους περί προστασίας προσωπικών δεδομένων μπορεί να οδηγήσει σε σοβαρές συνέπειες για τους οργανισμούς, συμπεριλαμβανομένων προστίμων, νομικών διεκδικήσεων και βλάβης της φήμης. Στο πλαίσιο του GDPR, για παράδειγμα, τα πρόστιμα μπορούν να φτάσουν το 4% του ετήσιου παγκόσμιου κύκλου εργασιών της επιχείρησης ή 20 εκατομμύρια ευρώ, ανάλογα με το ποιο είναι υψηλότερο. Επιπλέον, η μη συμμόρφωση μπορεί να οδηγήσει σε ζημία της εμπιστοσύνης των πελατών και του κοινού, καθώς και σε πιθανή απώλεια επιχειρηματικών ευκαιριών.

Για να αποφευχθούν αυτές οι συνέπειες, οι οργανισμοί πρέπει να ενσωματώσουν την προστασία δεδομένων σε όλα τα επίπεδα της λειτουργίας τους και να διασφαλίσουν την τακτική αναθεώρηση και ενημέρωση των πολιτικών και διαδικασιών τους για την προστασία

δεδομένων. Η στενή συνεργασία με νομικούς συμβούλους και ειδικούς στην προστασία δεδομένων μπορεί να βοηθήσει τους οργανισμούς να παραμείνουν ενημερωμένοι σχετικά με τις τρέχουσες και μελλοντικές απαιτήσεις συμμόρφωσης και να λάβουν τα κατάλληλα μέτρα για τη διασφάλιση της συνεχούς προστασίας των προσωπικών δεδομένων.

- Βέλτιστες Πρακτικές

Η προστασία των προσωπικών δεδομένων αποτελεί ένα ζωτικό στοιχείο για την ασφάλεια των ατόμων και την ενίσχυση των δημοκρατικών διαδικασιών. Η διασφάλιση της ιδιωτικότητας, ενώ παράλληλα επιτρέπεται η κοινή χρήση δεδομένων, απαιτεί την εφαρμογή στρατηγικών διακυβέρνησης δεδομένων, οι οποίες περιλαμβάνουν τεχνολογίες ενίσχυσης της ιδιωτικής ζωής (Privacy Enhancing Technologies - PETs) και στρατηγικές σχεδιασμού απορρήτου (Danezis et al., 2015). Παρ' όλο που οι PETs υπάρχουν, όπως η κρυπτογράφηση, δεν χρησιμοποιούνται ευρέως λόγω έλλειψης εναρμονισμένων προσεγγίσεων στην αντιμετώπιση παραβιάσεων δεδομένων (Danezis et al., 2015; Malatras et al., 2017). Η έλλειψη αυτή υποδηλώνει την ανάγκη για συστηματικές προσεγγίσεις και την αναζήτηση βέλτιστων πρακτικών για την ενίσχυση της συνεργασίας και την επικοινωνία μεταξύ των κρατών μελών.

- Διασφάλιση Συμμόρφωσης με το Νομοθετικό Πλαίσιο

Για τη διασφάλιση της συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) και άλλους σχετικούς νόμους, οι οργανισμοί πρέπει να επιδεικνύουν λογοδοσία μέσω της αξιολόγησης των παρόχων υπηρεσιών που διαχειρίζονται τα δεδομένα τους, διασφαλίζοντας ότι συμμορφώνονται με τις απαιτήσεις προστασίας δεδομένων (Hoofnagle et al., 2019). Η χρήση πλαισίων συμβατότητας με το απόρρητο και ο σχεδιασμός αρχιτεκτονικών λογισμικού που σέβονται την ιδιωτικότητα είναι ζωτικής σημασίας για την ενίσχυση της διακυβέρνησης δεδομένων (Canedo et al., 2019; Anthonysamy et al., 2017; Gellert, 2018; Hjerppe et al., 2019). Οι οργανισμοί πρέπει επίσης να διορίζουν έναν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer - DPO) για να διασφαλίζουν την επιτήρηση και την εφαρμογή των πολιτικών προστασίας δεδομένων (Stuurman & Kamara, 2016).

- Συνέπειες της Μη Συμμόρφωσης

Η μη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων μπορεί να επιφέρει σημαντικές νομικές και οικονομικές συνέπειες, συμπεριλαμβανομένων προστίμων, δικαστικών διαδικασιών και ζημίας της φήμης. Σύμφωνα με τον GDPR, τα πρόστιμα

μπορούν να ανέλθουν έως και στο 4% του ετήσιου παγκόσμιου κύκλου εργασιών της επιχείρησης ή 20 εκατομμύρια ευρώ, ανάλογα με το ποιο είναι το υψηλότερο (Stuurman & Kamara, 2016). Η ζημία της εμπιστοσύνης των πελατών και της εικόνας της επιχείρησης στο κοινό, καθώς και η πιθανή απώλεια επιχειρηματικών ευκαιριών, αποτελούν επίσης σημαντικές συνέπειες της μη συμμόρφωσης.

Για την πρόληψη των ανωτέρω συνεπειών, είναι κρίσιμο για τους οργανισμούς να αναπτύξουν και να εφαρμόσουν μια στρατηγική ολοκληρωμένης προστασίας δεδομένων που να περιλαμβάνει εκτενείς διαδικασίες ελέγχου, εκπαίδευσης προσωπικού, και συνεχή αξιολόγηση και αναθεώρηση των πολιτικών ασφαλείας δεδομένων. Η ενσωμάτωση της αρχής του "Privacy by Design" στην αρχιτεκτονική των συστημάτων και των εφαρμογών, δηλαδή η ενσωμάτωση της προστασίας των δεδομένων από την αρχική φάση σχεδιασμού, καθώς και η εφαρμογή τεχνολογιών που διασφαλίζουν την ασφάλεια των δεδομένων, όπως η κρυπτογράφηση και η ταυτοποίηση δύο παραγόντων, είναι επίσης απαραίτητες πρακτικές (Danezis et al., 2015).

Επιπλέον, η εφαρμογή ενός συστήματος διαχείρισης περιστατικών παραβίασης δεδομένων είναι ζωτικής σημασίας για την άμεση αντίδραση και αντιμετώπιση τυχόν παραβιάσεων, μειώνοντας έτσι τις πιθανές ζημίες. Η συνεχής επικοινωνία και συνεργασία με τις αρχές προστασίας δεδομένων, καθώς και η ενημέρωση των ενδιαφερομένων για τις πρακτικές ασφαλείας και τις πολιτικές προστασίας δεδομένων, ενισχύουν τη διαφάνεια και την εμπιστοσύνη (Gellert, 2018).

Τέλος, η κατάρτιση και η συνεχής εκπαίδευση του προσωπικού σε θέματα ασφαλείας και προστασίας προσωπικών δεδομένων αποτελούν κρίσιμο παράγοντα για την πρόληψη ανθρώπινων λαθών και την ενίσχυση της κουλτούρας ασφαλείας εντός του οργανισμού. Η συνειδητοποίηση των υπαλλήλων σχετικά με τις πρακτικές ασφαλείας και τη σημασία της προστασίας των δεδομένων συμβάλλει σημαντικά στην προάσπιση του απορρήτου και την αποφυγή παραβιάσεων δεδομένων (Hjerppe et al., 2019).

Συνοψίζοντας, η εφαρμογή των βέλτιστων πρακτικών για την προστασία προσωπικών δεδομένων απαιτεί μια ολοκληρωμένη προσέγγιση που περιλαμβάνει τεχνολογικές, οργανωτικές και νομικές στρατηγικές, καθώς και τη δέσμευση για συνεχή βελτίωση και ενημέρωση στο δυναμικό περιβάλλον της προστασίας δεδομένων.

Κεφάλαιο 2ο: Σημασία της Προστασίας των Δεδομένων στις Επιχειρήσεις

Όπως αναφέρθηκε προηγουμένως, η προστασία δεδομένων είναι μια κρίσιμη πτυχή της διατήρησης του απορρήτου στην ψηφιακή εποχή. Η ιστορία της νομοθεσίας περί απορρήτου χρονολογείται από τη δεκαετία του 1960, όταν η Ευρώπη και οι Ηνωμένες Πολιτείες θεσπίζουν νομοθεσία για την προστασία των προσωπικών δεδομένων. Έκτοτε, διάφορες πρωτοβουλίες έχουν ληφθεί, συμπεριλαμβανομένων των οδηγιών του Οργανισμού για την Οικονομική Συνεργασία και την Ανάπτυξη (ΟΟΣΑ), της Οδηγίας 95/46/ΕΚ, και πλέον του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση. Ο GDPR έχει πρακτικές συνέπειες για τα μέτρα προστασίας της ιδιωτικής ζωής. Απαιτεί από τους οργανισμούς να εφαρμόζουν τόσο οργανωτικά όσο και τεχνικά μέτρα προστασίας της ιδιωτικής ζωής. Η συμμόρφωση με τον GDPR και άλλους νόμους περί προστασίας δεδομένων απαιτεί σημαντικό χρόνο, σχεδιασμό, εκπαίδευση, καθώς και οικονομικούς και ανθρώπινους πόρους (Tikkinen-Piri et al., 2018).

Ο GDPR στοχεύει στο να παρέχει στα άτομα καλύτερο έλεγχο και διαχείριση των προσωπικών τους δεδομένων, να ενισχύσει την εμπιστοσύνη τους στις εταιρείες συλλογής δεδομένων και να εναρμονίσει την προστασία δεδομένων σε ολόκληρη την ΕΕ. Ο GDPR επιφέρει επίσης βασικές αλλαγές στις τρέχουσες πρακτικές προστασίας δεδομένων των εταιρειών, οι οποίες απαιτούν σημαντικούς οικονομικούς και ανθρώπινους πόρους, συμπεριλαμβανομένης της εκπαίδευσης των εργαζομένων. Οι αλλαγές που εισάγονται από τον GDPR αποσκοπούν στο να ωφελήσουν τις εταιρείες προσφέροντας συνέπεια στις δραστηριότητες και τις υποχρεώσεις προστασίας δεδομένων. Ωστόσο, η εφαρμογή του απορρήτου δεδομένων στις επιχειρηματικές λειτουργίες είναι συχνά προκλητική και απαιτεί μια προληπτική. Καλύπτει διάφορες πτυχές, όπως η ευαισθητοποίηση, η εκπαίδευση, η υιοθέτηση προστατευτικών μέτρων και η τεκμηρίωση των εργασιών επεξεργασίας (Tikkinen-Piri et al., 2018).

Τέλος, οι πεποιθήσεις των καταναλωτών σχετικά με την προστασία της ιδιωτικής ζωής επηρεάζονται από το περιβάλλον και τις συνθήκες. Συνεπώς, απαιτείται η ανάπτυξη ενός πλαισίου για τον διάλογο μεταξύ οργανισμών και καταναλωτών στο ηλεκτρονικό εμπόριο B2C, το οποίο θα πρέπει να ενσωματώνει ακαδημαϊκούς ερευνητές, παροχείς ηλεκτρονικού

εμπορίου, νομοθέτες, αυτορυθμιστές της βιομηχανίας και σχεδιαστές τεχνολογιών που ενισχύουν την προστασία της ιδιωτικής ζωής.

Μια στρατηγική προστασίας δεδομένων αποτελεί ουσιαστικό στοιχείο στα συστήματα διαχείρισης πληροφοριών κάθε οργανισμού. Κατά τον σχεδιασμό αυτής της στρατηγικής, πρέπει να δοθεί έμφαση στον σεβασμό του απορρήτου από την αρχή της διαδικασίας και να εξασφαλιστεί η ασφάλεια των δεδομένων. Είναι ουσιώδες να περιορίσουμε την ποσότητα των προσωπικών δεδομένων που συλλέγονται και να διασφαλίσουμε την τακτική παρακολούθηση και αξιολόγηση των προστατευτικών μέτρων. Η διαφάνεια και η φιλικότητα προς τους χρήστες πρέπει να είναι βασικές αρχές της στρατηγικής προστασίας δεδομένων, ενώ πρέπει να λαμβάνονται τόσο οργανωτικά όσο και τεχνικά μέτρα που να είναι κατάλληλα για το συγκεκριμένο πλαίσιο και σκοπό της επεξεργασίας δεδομένων. Οι επτά βασικές αρχές προστασίας δεδομένων του GDPR πρέπει να τηρούνται πιστά.

Άλλα σημαντικά στοιχεία μιας στρατηγικής προστασίας δεδομένων περιλαμβάνουν τη λογοδοσία, τον περιορισμό σκοπού, την ακεραιότητα και το απόρρητο των προσωπικών δεδομένων, την ακρίβεια των δεδομένων, τη νομιμότητα, τη δικαιοσύνη και τη διαφάνεια στη συλλογή και χρήση δεδομένων. Επίσης, η ψευδωνυμοποίηση και η ανωνυμοποίηση δεδομένων αποτελούν σημαντικό κομμάτι της στρατηγικής προστασίας δεδομένων, καθώς και η επίτευξη ισορροπίας μεταξύ διατήρησης του απορρήτου και χρησιμοποίησης των δεδομένων. Τέλος, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να λάβει τεχνικά και οργανωτικά μέτρα πριν ξεκινήσει οποιαδήποτε επεξεργασία δεδομένων, προκειμένου να διευκολύνει τη συμμόρφωση με τις αρχές προστασίας δεδομένων (Stalla-Bourdillon et al., 2019).

2.1 Επιπτώσεις των παραβιάσεων δεδομένων

Οι παραβιάσεις δεδομένων αποτελούν μια αυξανόμενη ανησυχία τόσο για τα άτομα όσο και για τους οργανισμούς. Η συχνότητα και η σοβαρότητα των παραβιάσεων διαφέρουν ανάλογα με το μέγεθος των οργανισμών, με τους μεγαλύτερους οργανισμούς να εκτίθενται σε πιο σοβαρές επιθέσεις. Πρόσφατες αναφορές δείχνουν ότι το μέγιστο μέγεθος παραβίασης αυξάνεται συνεχώς και αναμένεται να αυξηθεί ακόμη περισσότερο στα επόμενα χρόνια (Wheatley et al., 2016). Αυτές οι παραβιάσεις μπορούν να έχουν σοβαρές επιπτώσεις, συμπεριλαμβανομένης της μαζικής απάτης ταυτότητας, που μπορεί να προκαλέσει

οικονομικές απώλειες τόσο σε άτομα όσο και σε οργανισμούς (Wheatley et al., 2016; Hammouchi et al., 2019).

Το οικονομικό κόστος των παραβιάσεων δεδομένων είναι σημαντικό και μπορεί να έχει σημαντικές επιπτώσεις στους οργανισμούς και την παγκόσμια οικονομία. Οι δαπάνες περιλαμβάνουν την διερεύνηση περιστατικών, τη διαχείριση κρίσεων, ρυθμιστικές και βιομηχανικές κυρώσεις, ομαδικές αγωγές και το κόστος ευκαιρίας. Είναι σημαντικό να σημειωθεί ότι το κόστος ανά εγγραφή, που είναι μια συνηθισμένη μέτρηση, δεν αντικατοπτρίζει πλήρως το συνολικό οικονομικό κόστος μιας παραβίασης δεδομένων, καθώς υπάρχουν αποκλίσεις στο κόστος ανά εγγραφή. Σημαντικά επίσης είναι τα άμεσα και έμμεσα κόστη, όπως οι απώλειες φήμης, που είναι δύσκολο να μετρηθούν πλήρως. Τα συνολικά κόστη μιας παραβίασης δεδομένων έχουν επίπτωση όχι μόνο στους οργανισμούς αλλά και στην κοινωνία συνολικά, καθώς μπορούν να επηρεάσουν την εμπιστοσύνη και την οικονομία. Η ενίσχυση της κυβερνοασφάλειας και η υιοθέτηση βελτιωμένων πρακτικών ασφαλείας μπορεί να βοηθήσει στη μείωση του κινδύνου παραβίασης δεδομένων (Algarni et al., 2021).

Οι παραβιάσεις δεδομένων μπορούν να έχουν σημαντικές επιπτώσεις στις επιχειρήσεις, ιδιαίτερα στον κλάδο της φιλοξενίας, ο οποίος έχει κερδίσει αυξανόμενο ενδιαφέρον σε αυτό το θέμα (Gao et al., 2021). Η επίδραση των παραβιάσεων δεδομένων στην εμπιστοσύνη των πελατών και την επιχειρηματική φήμη είναι κρίσιμη (Gao et al., 2021). Όταν συμβαίνει μια παραβίαση δεδομένων, μπορεί να υπονομεύσει την εμπιστοσύνη των πελατών σε μια επιχείρηση και να επηρεάσει αρνητικά τη φήμη της (Juma'h & Alnsour, 2020). Οι καταναλωτές τείνουν να έχουν παρόμοιες αντιδράσεις απέναντι σε εταιρείες με τις οποίες έχουν σχέσεις, και οι αξιολογήσεις και οι προθέσεις συμπεριφοράς τους προς αυτές τις εταιρείες επηρεάζονται από τις προσπάθειές τους να αντιμετωπίσουν τις παραβιάσεις δεδομένων. Ο σωστός χειρισμός των παραβιάσεων δεδομένων μπορεί να αυξήσει την ικανοποίηση των πελατών και την προθυμία να μοιραστούν θετικές εντυπώσεις, ενώ ο εσφαλμένος χειρισμός τους μπορεί να οδηγήσει σε αρνητικές εντυπώσεις και να αναγκάσει τους πελάτες να αναζητήσουν αποζημίωση (Gao et al., 2021).

Οι παραβιάσεις δεδομένων μπορούν να έχουν νομικές, κοινωνικές και οικονομικές επιπτώσεις (Juma'h & Alnsour, 2020). Επομένως, η κατανόηση της επίδρασης της αγνώστου κατάστασης στη συμπεριφορά των καταναλωτών είναι απαραίτητη (Gao et al., 2021). Η έρευνα προτείνει ένα πλαίσιο που ενσωματώνει τα αποτελέσματα της σταθερότητας των

σφαλμάτων, της αντίληψης της επωνυμίας και των κανόνων σχέσεων σχετικά με τον τρόπο με τον οποίο οι παραβιάσεις δεδομένων επηρεάζουν την εμπιστοσύνη των πελατών και την επιχειρηματική φήμη. Στο μέλλον, η έρευνα μπορεί να επικεντρωθεί στον έλεγχο των υποθέσεων που παρουσιάζονται στο άρθρο και στην εξέταση των όρων υπό τους οποίους επηρεάζει η παραβίαση δεδομένων την εμπιστοσύνη των πελατών και την επιχειρηματική φήμη (Gao et al., 2021).

2.2 Επίδραση στην εμπιστοσύνη των πελατών

Στον τομέα των διαδικτυακών αγορών, οι πολιτικές προστασίας δεδομένων και απορρήτου ασκούν κρίσιμο ρόλο στην καταξίωση της εμπιστοσύνης των πελατών. Οι πελάτες εμπιστεύονται περισσότερο ιστότοπους που παρέχουν ασφαλείς σελίδες και έχουν διακριτικές πολιτικές προστασίας δεδομένων/απορρήτου. Αντίστροφα, ασαφείς πολιτικές προστασίας δεδομένων/απορρήτου αποθαρρύνουν τους πελάτες από τη δημοσιοποίηση των προσωπικών τους δεδομένων κατά τις αγορές στο διαδίκτυο. Επιπλέον, οι πελάτες είναι επιφυλακτικοί στο να αποκαλύπτουν τα δεδομένα τους σε τρίτους από τον πωλητή (Okeke et al., 2013).

Οι ανησυχίες σχετικά με το απόρρητο αναγνωρίζονται ως ένα από τα σημαντικότερα εμπόδια για την ανάπτυξη του ηλεκτρονικού εμπορίου. Είναι προφανές ότι οι ανησυχίες αυτές μπορεί να αποτελέσουν κύρια αιτία για την απώλεια εμπιστοσύνης μεταξύ των καταναλωτών και των επιχειρήσεων. Όταν προκύπτουν προβλήματα απορρήτου, η εμπιστοσύνη μεταξύ πελατών και επιχειρήσεων υπονομεύεται, με αρνητικές επιπτώσεις στην πίστη των πελατών και την επιχειρηματική απόδοση (Midha, 2012). Επομένως, η εφαρμογή βέλτιστων πρακτικών για την προστασία δεδομένων και το απόρρητο απαιτεί μια συνολική προσέγγιση που περιλαμβάνει τεχνολογικές, οργανωτικές και νομικές στρατηγικές, καθώς και δέσμευση για συνεχή βελτίωση και ενημέρωση σε ένα δυναμικό περιβάλλον προστασίας δεδομένων.

Συνεπώς, η απώλεια εμπιστοσύνης των πελατών έχει αρνητικές συνέπειες στη μελλοντική συμπεριφορά των καταναλωτών. Η εμπιστοσύνη είναι αναγκαία για τη δημιουργία αφοσίωσης των πελατών, αλλά η απώλειά της μπορεί να οδηγήσει σε μείωση αυτής της αφοσίωσης και της πιστοποίησης. Οι πελάτες που αντιμετωπίζουν προβλήματα με την ασφάλεια και την προστασία των δεδομένων μπορεί να αναζητούν εναλλακτικές λύσεις ή να

μειώσουν τη συχνότητα των αγορών τους στο διαδίκτυο. Αυτό μπορεί να έχει ως αποτέλεσμα απώλεια εσόδων και κερδών για τις επιχειρήσεις (Aldboush & Ferdous, 2023).

Συνοψίζοντας, η προστασία των δεδομένων και το απόρρητο είναι κρίσιμοι παράγοντες που επηρεάζουν την εμπιστοσύνη των πελατών στο διαδίκτυο. Η εμπιστοσύνη αποτελεί θεμέλιο λίθο για την επιτυχία των επιχειρήσεων στον τομέα του ηλεκτρονικού εμπορίου και η παραβίαση της προστασίας δεδομένων μπορεί να έχει σοβαρές συνέπειες για την επιχείρηση. Επομένως, οι επιχειρήσεις πρέπει να επενδύουν στην ανάπτυξη και εφαρμογή αποτελεσματικών πολιτικών προστασίας δεδομένων και απορρήτου για να διασφαλίσουν την εμπιστοσύνη των πελατών και την επιτυχία τους στον διαδικτυακό χώρο.

2.3 Σχέση με την επιχειρηματική επίδοση και τη φήμη

Η προστασία των δεδομένων επηρεάζει σημαντικά την απόδοση των επιχειρήσεων στη σύγχρονη εποχή. Με την αύξηση του κόστους συντήρησης παραδοσιακών εσωτερικών συστημάτων πληροφοριών, πολλές επιχειρήσεις απευθύνονται στο cloud computing για την αποθήκευση δεδομένων τους. Παρόλο που το cloud computing προσφέρει ευελιξία και κλιμάκωση, μπορεί επίσης να εκθέσει τα δεδομένα σε υψηλότερους κινδύνους ασφάλειας. Αυτή η μετάβαση συχνά οδηγεί σε απώλεια ελέγχου επί των μέτρων ασφαλείας, προκαλώντας ανησυχίες (Wang et al., 2020).

Παρά τις προκλήσεις, η προστασία δεδομένων μπορεί να βελτιώσει την επιχειρηματική απόδοση. Η έλλειψη προστασίας δεδομένων μπορεί να επηρεάσει αρνητικά την εμπιστοσύνη στο ηλεκτρονικό εμπόριο, μειώνοντας τις ψηφιακές συναλλαγές. Αντίθετα, αποτελεσματικά μέτρα προστασίας δεδομένων μπορούν να αυξήσουν την αξιοπιστία στο ηλεκτρονικό εμπόριο και να βελτιώσουν την επιχειρηματική απόδοση (Frik & Mittone, 2019).

Ωστόσο, παραβιάσεις δεδομένων μπορούν να έχουν σοβαρές μακροπρόθεσμες επιπτώσεις στη φήμη των επιχειρήσεων. Η αρνητική κοινωνική αντίδραση και η απώλεια φήμης στα μέσα κοινωνικής δικτύωσης μπορεί να είναι δυσμενείς (Syed, 2019). Η πρόληψη και η αποτελεσματική αντιμετώπιση των παραβιάσεων δεδομένων είναι κρίσιμες για τη διατήρηση της επιχειρηματικής φήμης στο μακροπρόθεσμο (Gao et al., 2021).

Για να διατηρήσουν υψηλά πρότυπα προστασίας δεδομένων και να προστατεύσουν τη φήμη τους, οι επιχειρήσεις πρέπει να λάβουν υπόψη τις ακόλουθες στρατηγικές και πρακτικές:

1. Εφαρμογή Σύγχρονων Μέσων Προστασίας Δεδομένων (Susanto et al., 2021):

- Χρήση λογισμικού προστασίας από ιούς και τειχών προστασίας για αποτροπή επιθέσεων.

- Χρήση βιομετρικών συσκευών ασφαλείας για την ενίσχυση των συστημάτων.

- Χρήση μοναδικών κωδικών πρόσβασης για προστασία των πληροφοριών.

2. Συμμόρφωση με Διεθνή Πρότυπα (Susanto et al., 2021):

- Συμμόρφωση με διεθνή πρότυπα που ρυθμίζουν τη χρήση της τεχνολογίας και των συστημάτων πληροφοριών.

3. Περιορισμός Πρόσβασης (Susanto et al., 2021):

- Περιορισμός του αριθμού των ατόμων που έχουν πρόσβαση στο σύστημα.

- Διάθεση διαφορετικών επιπέδων εξουσιοδότησης βάση των ρόλων.

4. Διαφάνεια (Abdulsalam & Hedabou, 2021):

- Ενημέρωση των πελατών σχετικά με τις πρακτικές δεδομένων.

- Παροχή σαφών και προσβάσιμων πολιτικών απορρήτου.

5. Αντιμετώπιση Κριτικών και Σχολίων (Susanto et al., 2021):

- Εξυπηρέτηση των πελατών μέσω των μέσων κοινωνικής δικτύωσης με επίγνωση των κινδύνων αρνητικών κριτικών και σχολίων.

Επιπλέον, οι επιχειρήσεις πρέπει να εφαρμόζουν συνεχείς αξιολογήσεις και βελτιώσεις στα συστήματά τους για τη διατήρηση υψηλών προτύπων προστασίας δεδομένων (Abdulsalam & Hedabou, 2021). Τονίζεται ότι οι παραβιάσεις της ασφάλειας δεδομένων μπορούν να οδηγήσουν σε μείωση της ποιότητας των υπηρεσιών και της ικανοποίησης των πελατών, με αρνητικές επιπτώσεις στη φήμη της επιχείρησης (Susanto et al., 2021).

Συνοψίζοντας, η προστασία των δεδομένων και η διατήρηση υψηλών προτύπων προστασίας αποτελούν ζωτικής σημασίας πτυχές για τη διατήρηση της φήμης των επιχειρήσεων στον σύγχρονο ψηφιακό κόσμο.

Κεφάλαιο 3ο: Κίνδυνοι και Προκλήσεις Προστασίας των Δεδομένων στις Επιχειρήσεις

Η προστασία δεδομένων στον επιχειρηματικό τομέα αποτελεί μια ουσιαστική διαδικασία που απαιτεί την εφαρμογή τόσο προληπτικών όσο και αντιδραστικών στρατηγικών. Η επιτυχία στην προστασία των δεδομένων επιτυγχάνεται μέσω της ολοκληρωμένης διαχείρισης του κύκλου ζωής τους, λαμβάνοντας υπόψη τις απαιτήσεις που αφορούν τα επίπεδα συμφωνητικών επιδόσεων (Service Level Agreements, SLA) και υπερβαίνοντας τις παραδοσιακές μεθόδους όπως το Redundant Array of Independent Disks (RAID), η διαθεσιμότητα, η αναπαραγωγή, τα στιγμιότυπα ή τα αντίγραφα ασφαλείας. Απαιτείται μια προσαρμοσμένη προσέγγιση βασισμένη στην κρισιμότητα των δεδομένων και τις επιχειρηματικές απαιτήσεις, όπως τονίζεται από τον De Guise (2017).

Αυτό περιλαμβάνει την ανάπτυξη τεχνολογιών και διαδικασιών που επιτρέπουν τη συνέχεια, την κίνηση και την επεξεργασία δεδομένων, συμβάλλοντας στη βελτιστοποίηση του κόστους και την αξιοποίηση των επενδύσεων πληροφορικής (De Guise, 2017). Επιπρόσθετα, η εμπειρία και η κατανόηση των τεχνολογιών και των διαδικασιών που χρησιμοποιούνται για τη συλλογή και επεξεργασία προσωπικών δεδομένων είναι κρίσιμης σημασίας για τη συμμόρφωση και τη διαχείριση κινδύνου (Ezor, 2012).

Η σημασία της προστασίας δεδομένων καθίσταται ιδιαίτερα εμφανής στον τομέα των χρηματοοικονομικών υπηρεσιών, όπου τα οικονομικά αρχεία αντιπροσωπεύουν ένα από τα πιο ευαίσθητα στοιχεία για τους καταναλωτές. Οι εταιρείες είναι υποχρεωμένες να συμμορφώνονται με τις Οκτώ Αρχές του Νόμου για την Προστασία Δεδομένων και να εξασφαλίζουν την προστασία του κύκλου ζωής των πελατών, από την αρχική επαφή έως την αναζήτηση επιπλέον επιχειρηματικών ευκαιριών. Η Αρχή Χρηματοοικονομικών Υπηρεσιών (Financial Services Authority, FSA) διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της συμμόρφωσης με αυτούς τους κανονισμούς, και η μη συμμόρφωση μπορεί να έχει σημαντικές συνέπειες (Tikkinen-Piri et al., 2018).

Οι νομικοί και ηθικοί παράγοντες που συνδέονται με την προστασία δεδομένων απαιτούν από τις επιχειρήσεις να εφαρμόζουν ασφαλείς και νόμιμες μεθόδους συλλογής, αποθήκευσης και κοινοποίησης δεδομένων. Η τήρηση των κανονισμών και των μέτρων προστασίας των προσωπικών πληροφοριών είναι κρίσιμη για την αποφυγή νομικών επιπλοκών και τη διασφάλιση της ηθικής συμμόρφωσης. Ο σεβασμός των δικαιωμάτων των ατόμων σε ιδιωτικότητα είναι θεμελιώδης, και οι επιχειρήσεις πρέπει να λαμβάνουν υπόψη τις νομικές και ηθικές πτυχές που σχετίζονται με την προστασία δεδομένων για την ενίσχυση της εμπιστοσύνης των πελατών. Οι προκλήσεις που σχετίζονται με την παραβίαση δεδομένων απαιτούν την εφαρμογή μέτρων για τον μετριασμό της βλάβης στους πελάτες και την τήρηση της ισχύουσας νομοθεσίας περί προστασίας δεδομένων (Taherdoost, 2023).

Οι επιχειρήσεις, κυρίως στον τομέα του ηλεκτρονικού εμπορίου, πρέπει να αντιμετωπίζουν τα νομικά και ηθικά διλήμματα που προκύπτουν από την προστασία δεδομένων και το απόρρητο, διασφαλίζοντας την προστασία της πνευματικής ιδιοκτησίας και την τήρηση των ευρωπαϊκών κανονισμών για την προστασία δεδομένων (Finn & Wright, 2016; Taherdoost, 2023). Η ενίσχυση της εμπιστοσύνης και η διασφάλιση της συμμόρφωσης με τις νομικές και ηθικές απαιτήσεις αποτελούν θεμελιώδη στόχους για τις επιχειρήσεις που δραστηριοποιούνται στον ψηφιακό κόσμο.

3.1 Κύριοι κίνδυνοι παραβίασης δεδομένων

Οι παραβιάσεις δεδομένων αναφέρονται σε περιστατικά όπου διακυβεύονται ιδιωτικές πληροφορίες υγείας, προσωπικά δεδομένα πελατών ή πνευματική ιδιοκτησία χωρίς άδεια (Eling & Loperfido, 2017). Αυτές οι παραβιάσεις έχουν αυξηθεί παρά τα μέτρα κυβερνοασφάλειας (Eling & Loperfido, 2017). Τα δεδομένα που παραβιάζονται μπορούν να οδηγήσουν σε νομικές, φήμης και οικονομικές ζημίες (Eling & Loperfido, 2017).

Οι επιχειρήσεις αντιμετωπίζουν κινδύνους παραβίασης δεδομένων που σχετίζονται με την υγεία και τα προσωπικά δεδομένα (Algarni et al., 2021). Η πρόληψη τους απαιτεί την καλύτερη κατανόηση των τύπων παραβιάσεων και των παραγόντων κινδύνου (Sarabi et al., 2016). Οι εξωτερικοί και εσωτερικοί παράγοντες μπορούν να συμβάλλουν στον κίνδυνο παραβίασης δεδομένων (Algarni et al., 2021).

Οι επιχειρήσεις πρέπει να λαμβάνουν μέτρα για την προστασία των δεδομένων και την αντιμετώπιση των πιθανών παραβιάσεων (Chen et al., 2023). Αυτά τα μέτρα μπορούν να περιλαμβάνουν την ενίσχυση της κυβερνοασφάλειας και την καλύτερη διαχείριση του κινδύνου. Είναι σημαντικό να γίνει κατανοητό ότι καμία επιχείρηση δεν είναι απρόσβλητη από παραβιάσεις δεδομένων, αλλά μπορεί να προετοιμαστεί για να τις αντιμετωπίσει αποτελεσματικά (Sarabi et al., 2016).

Οι επιπτώσεις της παραβίασης δεδομένων στις επιχειρήσεις εκτείνονται σε οικονομικές, φημολογικές, λειτουργικές και ρυθμιστικές συνέπειες, με σημαντικό άμεσο και έμμεσο κόστος που μπορεί να απειλήσει την επιβίωση και την ανταγωνιστικότητά τους (Ibrahim et al., 2020). Μια αρνητική αντίδραση της αγοράς, που οδηγεί σε απώλεια πωλήσεων και κερδών, είναι μια συνήθης συνέπεια, όπως και η βλάβη της φήμης και η απώλεια της εμπιστοσύνης των πελατών λόγω δυσμενούς δημοσιότητας.

Οι επιχειρήσεις μπορεί επίσης να επιβαρυνθούν με σημαντικό κόστος για την αποζημίωση τρίτων για ζημίες που προκύπτουν από παραβίαση δεδομένων και να αντιμετωπίσουν πρόστιμα και περιορισμούς λόγω μη συμμόρφωσης με τις απαιτήσεις ασφαλείας. Η αύξηση στις γνωστοποιήσεις παραγόντων κινδύνου για την κυβερνοασφάλεια μετά από παραβίαση δεδομένων σχετίζεται με μια μη μηδενική αντίδραση της αγοράς, ενώ οι εταιρείες που αποκαλύπτουν στρατηγικές μετριασμού κινδύνου είναι λιγότερο πιθανό να υποστούν μελλοντικές παραβιάσεις (Chen et al., 2023).

3.2 Προκλήσεις στη Διαχείριση και Προστασία των Προσωπικών Δεδομένων

Σχετικά με τις προκλήσεις στη διαχείριση και προστασία των προσωπικών δεδομένων, οι επιχειρήσεις αντιμετωπίζουν σημαντικά εμπόδια, ειδικά με την εισαγωγή του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) (Grundstrom et al., 2019). Οι προκλήσεις αυτές περιλαμβάνουν την πολυπλοκότητα των δεδομένων, την ενοποίηση συστημάτων, τη διαφάνεια διαδικασιών και τη λογοδοσία, ενώ οι εταιρείες πρέπει να αναλαμβάνουν ευθύνη για τη διαχείριση και την προστασία των προσωπικών δεδομένων (Butarbutar, 2020).

Η αντιμετώπιση της ορολογίας των προσωπικών και των ευαίσθητων προσωπικών δεδομένων, καθώς και η ασαφής αρχή της προστασίας δεδομένων σε ορισμένες χώρες, όπως η Ινδονησία, αποτελούν επιπλέον προκλήσεις (Butarbutar, 2020). Η εφαρμογή του GDPR έχει εισαγάγει αλλαγές στους οργανισμούς και τις πρακτικές τους, με τις προκλήσεις να εκφράζονται μέσω τεσσάρων διαστάσεων: Διαδικασία, Προστασία, Απόρρητο και Διάδοση (Grundstrom et al., 2019). Είναι απαραίτητο για τις επιχειρήσεις να αναπτύξουν κατάλληλα μέτρα για την αντιμετώπιση αυτών των προκλήσεων, ώστε να διασφαλίζεται η ασφαλής διαχείριση των προσωπικών δεδομένων.

Η πολυπλοκότητα των κανονισμών προστασίας δεδομένων αντιπροσωπεύει μια από τις σημαντικότερες προκλήσεις στη διαχείριση και την προστασία των προσωπικών δεδομένων εντός των οργανισμών. Η θέσπιση του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) επιφέρει σημαντικές αλλαγές στην επεξεργασία προσωπικών πληροφοριών, ενισχύοντας τα δικαιώματα των ατόμων εντός της Ευρωπαϊκής Ένωσης (de Carvalho et al., 2020). Αυτή η αλλαγή, παρόλο που ενισχύει την προστασία δεδομένων, προκαλεί σημαντικές προκλήσεις λόγω της αυξημένης πολυπλοκότητας και των απαιτήσεων για τους οργανισμούς, που πρέπει να αναπτύξουν ικανότητες επίγνωσης παραβίασης δεδομένων και να βελτιώσουν την ασφάλεια των πληροφοριών τους. Η αυξημένη χρήση ψηφιακών υπηρεσιών απαιτεί από τους οργανισμούς να εφαρμόζουν διαφορετικά εργαλεία, λύσεις και διαδικασίες για τη συμμόρφωση με το GDPR, καθώς και την ενσωμάτωση της προστασίας δεδομένων στις διαδικασίες τους (Kuner et al., 2015; de Carvalho et al., 2020).

Στο πλαίσιο της αντιμετώπισης των προκλήσεων στη διαχείριση και προστασία των προσωπικών δεδομένων, οι επιχειρήσεις μπορούν να επωφεληθούν από την ανάπτυξη Personal Data Stores (PDS), τα οποία παρέχουν στα άτομα τον έλεγχο των προσωπικών τους δεδομένων. Αυτή η προσέγγιση, μαζί με την εφαρμογή τεχνολογικών λύσεων που ενισχύουν το απόρρητο και την προστασία δεδομένων, μπορεί να βοηθήσει στην αντιμετώπιση των εξελισσόμενων απειλών και την εξασφάλιση συμμόρφωσης με τις νομοθετικές απαιτήσεις (Van Kleek & O'Hara, 2014).

Όσον αφορά τις βέλτιστες πρακτικές για την προστασία δεδομένων στις επιχειρήσεις, είναι κρίσιμης σημασίας η εφαρμογή ενός ισχυρού πλαισίου διακυβέρνησης δεδομένων, η

επιβολή πολιτικών και διαδικασιών προστασίας δεδομένων, και η χρήση τεχνολογίας κρυπτογράφησης για την προστασία των εμπιστευτικών δεδομένων. Η συνεχής ενημέρωση και δοκιμή των μέτρων ασφαλείας είναι απαραίτητη για την αποτελεσματική προστασία ενάντια στις νέες απειλές. Επιπλέον, η κοινή χρήση πληροφοριών μεταξύ των μελών των δικτύων εφοδιαστικής αλυσίδας πρέπει να γίνεται μόνο όταν υπάρχουν κατάλληλα μέτρα διακυβέρνησης δεδομένων και προστασίας (Fernando et al., 2018).

Η εφαρμογή αυτών των βέλτιστων πρακτικών μπορεί να προσφέρει πολλαπλά οφέλη, όπως αυξημένη παραγωγικότητα, βελτίωση της ποιότητας και αποτελεσματικότητας της επεξεργασίας προσωπικών δεδομένων, καθώς και τη διασφάλιση της συμμόρφωσης με τις νομοθετικές απαιτήσεις (Tikkinen-Piri et al., 2018). Αυτές οι πρακτικές μπορούν επίσης να προσφέρουν ανταγωνιστικό πλεονέκτημα και να βελτιώσουν την ικανοποίηση των πελατών, ενώ παράλληλα προστατεύουν τα δικαιώματα ιδιωτικής ζωής των ατόμων. Η εφαρμογή των βέλτιστων πρακτικών απαιτεί συνεχή επικαιροποίηση και προσαρμογή στις εξελισσόμενες τεχνολογίες και τις νομοθετικές αλλαγές, αλλά αποτελεί κρίσιμο στοιχείο για την επιτυχία και την ανταγωνιστικότητα των επιχειρήσεων στη σύγχρονη οικονομική και κοινωνική σκηνή.

Κεφάλαιο 4ο: Εφαρμογή της Προστασίας Δεδομένων στις Επιχειρήσεις

4.1 Στρατηγικές για την προστασία των προσωπικών δεδομένων

Η αναγκαιότητα της προστασίας των προσωπικών δεδομένων εντός του επιχειρηματικού πλαισίου αποτελεί ένα κρίσιμο ζήτημα, το οποίο απαιτεί μια ολοκληρωμένη προσέγγιση που να συνδυάζει προληπτικές και αντιδραστικές στρατηγικές. Οι επιχειρήσεις επιδιώκουν να προστατεύσουν τα δεδομένα μέσω της εφαρμογής τεχνολογιών όπως η πιστοποίηση ταυτότητας και η κρυπτογράφηση, διασφαλίζοντας ταυτόχρονα την ασφαλή αποθήκευση, πρόσβαση και διαχείριση των δεδομένων (Morey et al., 2015; Mubarak Alharbi et al., 2013). Η ανάπτυξη μιας στρατηγικής προστασίας δεδομένων πρέπει να προσαρμόζεται στις ειδικές ανάγκες και το επίπεδο ευαισθησίας των δεδομένων της κάθε επιχείρησης, αντιμετωπίζοντας τις συνεχώς αυξανόμενες απειλές που ενδέχεται να διαταράξουν την ασφάλεια των προσωπικών δεδομένων (Mubarak Alharbi et al., 2013).

4.1.1 Εφαρμογή Στρατηγικών Προστασίας Δεδομένων

Στη Μαλαισία, ο Νόμος για την Προστασία Προσωπικών Δεδομένων (Personal Data Protection Act, PDPA) του 2010 ορίζει ότι οι οργανισμοί πρέπει να δημοσιοποιούν τις πολιτικές απορρήτου τους για να προστατεύσουν τα προσωπικά δεδομένα των καταναλωτών. Η μελέτη που πραγματοποιήθηκε από τους Chua et al. (2017) αποκάλυψε διαφορές στα επίπεδα συμμόρφωσης μεταξύ κυβερνητικών και ιδιωτικών οργανισμών, με τους τελευταίους να εμφανίζουν υψηλότερα επίπεδα συμμόρφωσης. Τα ευρήματα αυτά ενισχύουν την ανάγκη για αποτελεσματικότερους μηχανισμούς επιβολής της συμμόρφωσης με τον PDPA στη Μαλαισία (Chua et al., 2017).

4.1.2 Βασικές Εκτιμήσεις Κατά την Εφαρμογή Στρατηγικών Προστασίας Δεδομένων

Κατά την εφαρμογή στρατηγικών προστασίας δεδομένων, οι επιχειρήσεις οφείλουν να λαμβάνουν υπόψη τους περιορισμούς και τις ευκαιρίες που παρέχουν οι νόμοι προστασίας δεδομένων, επιλέγοντας τις καταλληλότερες στρατηγικές για την αντιμετώπιση των

προκλήσεων (Martin et al., 2019). Η ρύθμιση προστασίας δεδομένων έχει σημαντικό αντίκτυπο στη λειτουργία των επιχειρήσεων, και η συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation, GDPR) αποτελεί κρίσιμη προτεραιότητα (Grundstrom et al., 2019).

Επιπροσθέτως, οι επιχειρήσεις πρέπει να εξετάσουν τη διαφάνεια και την ενδυνάμωση των χρηστών σχετικά με τη διαχείριση των προσωπικών τους δεδομένων, προσφέροντας υπηρεσίες που σέβονται το απόρρητο και την αυτοδιάθεση των χρηστών (Mantelero, 2013; Quach et al., 2022). Η κατανόηση των προκλήσεων που σχετίζονται με την ασφάλεια και το απόρρητο στα μεγάλα δεδομένα, καθώς και η εφαρμογή αποτελεσματικών στρατηγικών για την αντιμετώπιση αυτών των ζητημάτων, είναι ουσιώδης για τη διασφάλιση της ανταγωνιστικότητας και της επιβίωσης των επιχειρήσεων στην ψηφιακή εποχή (Georgiadis & Poels, 2021).

4.2 Εφαρμογή των αρχών της προστασίας δεδομένων στις επιχειρήσεις

4.2.1 Βασικές Αρχές Προστασίας Δεδομένων που Θα Πρέπει να Εφαρμόζονται από τις Επιχειρήσεις

Στη σύγχρονη εποχή, η προστασία δεδομένων και η ευρύτερη χρήση τους αποτελούν κρίσιμα ζητήματα για την αντιμετώπιση νέων προκλήσεων. Αναθεωρημένες αρχές προστασίας δεδομένων έχουν εισαχθεί για το καλό ατόμων, επιχειρήσεων και κοινωνιών. Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation, GDPR) παρέχει στις επιχειρήσεις τη δυνατότητα να αναγνωρίσουν την αξία των προσωπικών δεδομένων των πελατών τους (Hoofnagle et al., 2019). Οι επιχειρήσεις καλούνται να εφαρμόσουν μέτρα για τη διόρθωση των ανακριβειών στα προσωπικά δεδομένα και να προωθήσουν την ελεύθερη κυκλοφορία δεδομένων, προάγοντας έτσι την ανάπτυξη τους (Tikkinen-Piri et al., 2018). Είναι σημαντικό οι επιχειρήσεις να ακολουθούν τις κατευθυντήριες γραμμές προστασίας δεδομένων, ελέγχοντας τις επίσημες ειδοποιήσεις απορρήτου που δημοσιεύουν, προκειμένου να παρέχουν λεπτομερείς πληροφορίες σχετικά με τη χρήση των προσωπικών δεδομένων (Chua et al., 2017).

Μη συμμόρφωση με τις αρχές αυτές μπορεί να οδηγήσει σε οικονομικές κυρώσεις έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών ή 20 εκατομμύρια ευρώ. Για τη διευκόλυνση της συμμόρφωσης, οι διευθυντές ή οι υπεύθυνοι δεδομένων μπορούν να εφαρμόσουν την επίσημη ανάλυση εννοιών (Formal Concept Analysis, FCA) για την κατανόηση και την εφαρμογή των θεμελιωδών αρχών του DPA και του GDPR (Tamburri, 2020). Οι αλλαγές στη νομοθεσία επηρεάζουν τον τρόπο λειτουργίας των επιχειρήσεων, όπως στην περίπτωση των εταιρειών αποθήκευσης δεδομένων, οι οποίες πρέπει να τηρούν ειδικές αρχές προστασίας δεδομένων (Mondschein & Monda, 2019). Η διαρκής εποπτεία και διαφάνεια στις πρακτικές προστασίας δεδομένων είναι απαραίτητη για την αποφυγή παραβιάσεων και των σχετικών κυρώσεων (Alhadeff et al., 2012). Η εφαρμογή συνεκτικών κανόνων προστασίας δεδομένων είναι κρίσιμη για τη συμμόρφωση με τις νομοθετικές απαιτήσεις και την προστασία των προσωπικών δεδομένων των πελατών (Boban, 2016).

4.2.2 Εφαρμογή των Αρχών Προστασίας Δεδομένων στην Πράξη από τις Επιχειρήσεις

Οι επιχειρήσεις αντιμετωπίζουν πολλαπλές προκλήσεις κατά την εφαρμογή των αρχών προστασίας δεδομένων στην πράξη, ειδικά σε σχέση με την διαδικτυακή συναίνεση (Carolan, 2016). Οι κανονισμοί όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) της Ευρωπαϊκής Ένωσης (ΕΕ) παρουσιάζουν ένα περίπλοκο κανονιστικό πλαίσιο (Carolan, 2016; Tamburri, 2020). Η συμμόρφωση με τον GDPR απαιτεί σημαντική προσοχή, καθώς το κείμενό του απευθύνεται κυρίως σε νομικούς και υπεύθυνους πολιτικής και όχι σε μηχανικούς (Tamburri, 2020).

Η παραδοσιακή νομική προσέγγιση στη συναίνεση για την προστασία δεδομένων αντιμετωπίζει προβλήματα, καθώς τα άτομα μπορεί να μην κατανοούν πλήρως τις δραστηριότητες στις οποίες έχουν συναινέσει (Carolan, 2016). Η επίσημη ανάλυση εννοιών (Formal Concept Analysis, FCA) μπορεί να αποτελέσει εργαλείο για την κατανόηση και την εφαρμογή των αρχών του GDPR, βοηθώντας τις εταιρείες να αναπτύξουν συμβατά συστήματα και υπηρεσίες (Tamburri, 2020). Τα ζητήματα απορρήτου στα μεγάλα δεδομένα και η ανάγκη για ανάπτυξη στρατηγικών και πολιτικών προστασίας δεδομένων προσθέτουν στις προκλήσεις της εφαρμογής των αρχών προστασίας δεδομένων στις επιχειρήσεις (Carolan, 2016; Braun & Garriga, 2017). Εν τέλει, οι εταιρείες οφείλουν να υιοθετούν μια προληπτική προσέγγιση, εφαρμόζοντας βέλτιστες πρακτικές και τηρώντας τους σχετικούς

κανονισμούς και οδηγίες για την ασφάλεια και το απόρρητο των δεδομένων (Torra & Navarro-Arribas, 2016).

4.3 Παραδείγματα πρακτικών προστασίας

Η εφαρμογή αποτελεσματικών πρακτικών προστασίας δεδομένων αποτελεί κρίσιμο στοιχείο για τη διασφάλιση της ασφάλειας των ευαίσθητων πληροφοριών εντός μιας επιχείρησης. Μια σημαντική πρακτική στον τομέα αυτό είναι η Προστασία μέσω του Σχεδιασμού (Privacy by Design - PbD), η οποία προωθεί μια προληπτική προσέγγιση στην προστασία της ιδιωτικότητας (Tikkinen-Piri et al., 2018). Το PbD αναγνωρίζει την ανάγκη για συνεχή προσαρμογή στις απαιτήσεις της προστασίας δεδομένων, μεταβαίνοντας αποτελεσματικά σε βελτιωμένες μεθόδους προστασίας. Αυτό περιλαμβάνει την εφαρμογή αποτελεσματικών μεθόδων διαχείρισης κωδικών πρόσβασης και την εκτέλεση αξιολογήσεων επιπτώσεων στην προστασία δεδομένων (Ruivo et al., 2014). Επιπλέον, η διάκριση μεταξύ της ασφάλειας και της προστασίας δεδομένων είναι ουσιαστική, με την πρώτη να εστιάζει στην προστασία από μη εξουσιοδοτημένη πρόσβαση και τη δεύτερη στην προστασία από κακοδοχεία χρήση ευαίσθητων πληροφοριών (von Grafenstein et al., 2022).

Η εφαρμογή ολοκληρωμένων πολιτικών προστασίας δεδομένων, που περιλαμβάνουν λεπτομερείς οδηγίες για την ασφαλή διαχείριση επιχειρηματικών δεδομένων, κρίνεται απαραίτητη (Foulsham, 2019). Οι επιχειρήσεις οφείλουν να ενσωματώσουν τις βασικές αρχές προστασίας της ιδιωτικότητας, εξασφαλίζοντας την τήρηση των απαιτούμενων διασφαλίσεων για την ποιότητα και την ασφάλεια των δεδομένων (Cate, 2016). Οι εταιρείες που εφαρμόζουν αυτές τις πρακτικές μπορούν να αποφεύγουν νομικές ενέργειες για αθέμιτες πρακτικές ασφαλείας δεδομένων, να υποστηρίζουν ηθικές επιχειρηματικές πρακτικές και να αποτρέπουν την έκθεση σε πιθανή βλάβη (Ezor, 2012; Ferris, 2017).

Οι εν λόγω πρακτικές πρέπει να ευθυγραμμίζονται με τις καθιερωμένες αρχές προστασίας δεδομένων, προσφέροντας μια ολοκληρωμένη προστασία στα προσωπικά δεδομένα των ατόμων. Η Προστασία μέσω του Σχεδιασμού (PbD), για παράδειγμα, επιτυγχάνει ακριβώς αυτό, θέτοντας την προστασία της ιδιωτικότητας ως βασική προτεραιότητα στον σχεδιασμό νέων προϊόντων και υπηρεσιών (Tikkinen-Piri et al., 2018). Η συνεχής εποπτεία και διαφάνεια στις πρακτικές προστασίας δεδομένων, καθώς και η εφαρμογή συγκεκριμένων

πολιτικών που διασφαλίζουν την ασφαλή επεξεργασία και χρήση των επιχειρηματικών δεδομένων, είναι επίσης σύμφωνες με τις αρχές προστασίας δεδομένων (Foulsham, 2019). Οι επιχειρήσεις που εφαρμόζουν αυτές τις πρακτικές δεν μόνο προστατεύουν τα δεδομένα αλλά και ενισχύουν την εμπιστοσύνη και τη σχέση με τους πελάτες τους, διασφαλίζοντας την τήρηση των διατάξεων του GDPR και άλλων σχετικών κανονισμών (Tamburri, 2020).

Οι επιχειρήσεις που αναζητούν να βελτιώσουν τις πρακτικές προστασίας δεδομένων τους μπορούν να αντλήσουν σημαντικά διδάγματα από τα παραδείγματα αυτά. Η προτεραιοποίηση της προστασίας δεδομένων, η εφαρμογή αποτελεσματικών μεθόδων διαχείρισης και η τήρηση των νομοθετικών απαιτήσεων είναι κρίσιμα στοιχεία για την επίτευξη αυτού του στόχου. Οι επιχειρήσεις πρέπει να ενσωματώσουν τις αρχές προστασίας δεδομένων σε όλες τις λειτουργίες τους, να διασφαλίσουν την εφαρμογή των απαιτήσεων ασφαλείας και να αναπτύξουν ένα πολιτισμό εταιρικής ευθύνης και δέσμευσης για την προστασία των προσωπικών δεδομένων. Μέσω της εφαρμογής αυτών των πρακτικών, οι επιχειρήσεις μπορούν να ενισχύσουν την απόδοσή τους, να μειώσουν τους κινδύνους και να αυξήσουν την εμπιστοσύνη των πελατών τους στις δραστηριότητές τους.

Κεφάλαιο 5^{ο}: Νομικά Θέματα και Συμμόρφωση

5.1 Ανάλυση των νομικών πτυχών σχετικά με την προστασία των δεδομένων

Οι οργανισμοί ανά τον κόσμο είναι υποχρεωμένοι να ακολουθούν πολύπλοκες νομοθετικές διατάξεις σχετικά με την προστασία προσωπικών δεδομένων για την εξασφάλιση της ασφάλειας και του απορρήτου των πληροφοριών. Στον Καναδά, για παράδειγμα, οι οργανισμοί υπόκεινται στον Νόμο Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA), όπου αναλαμβάνουν την ευθύνη για τις προσωπικές πληροφορίες που διαχειρίζονται, συμπεριλαμβανομένης της μεταβίβασης σε τρίτους για επεξεργασία (Phillips, 2018). Αυτός ο νόμος είναι εμπνευσμένος από τις αρχές των κατευθυντήριων γραμμών του Οργανισμού για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ) σχετικά με την προστασία της ιδιωτικότητας (Phillips, 2018).

Εντός της Ευρωπαϊκής Ένωσης, ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) ορίζει το κανονιστικό πλαίσιο για την προστασία δεδομένων, με το Κεφάλαιο V να καθορίζει τις διατάξεις για τη διεθνή μεταφορά δεδομένων. Οι οργανισμοί πρέπει να ακολουθούν εγκεκριμένους κώδικες δεοντολογίας με δεσμευτικές και εκτελεστές δεσμεύσεις για την εφαρμογή κατάλληλων διασφαλίσεων (Phillips, 2018). Στις Ηνωμένες Πολιτείες, ο Νόμος Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας (HIPAA) του 1996 ρυθμίζει την προστασία των δεδομένων υγείας, απαιτώντας από τους οργανισμούς να προστατεύουν τα δεδομένα υγείας που διαχειρίζονται (Phillips, 2018).

Η Οδηγία της Ευρωπαϊκής Ένωσης για την Προστασία Δεδομένων (1995) και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Ευρωπαϊκή Ένωση, 2016) απαιτούν οποιαδήποτε μεταφορά σε χώρα εκτός ΕΕ να συμμορφώνεται με τις αποφάσεις επάρκειας που έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή (Phillips, 2018). Αυτό απαιτεί από τους οργανισμούς να παρακολουθούν συνεχώς την ισχύ των αποφάσεων επάρκειας για να διασφαλίσουν τη διαρκή συμμόρφωση με τις απαιτήσεις της ΕΕ.

Παράλληλα, ειδικά πλαίσια προστασίας δεδομένων για τον τομέα της υγείας και άλλους ειδικούς τομείς αναπτύσσονται σε διεθνές επίπεδο, όπως το Διεθνές Πρότυπο για την Προστασία του Απορρήτου και των Προσωπικών Πληροφοριών του Παγκόσμιου

Οργανισμού Αντιντόπινγκ (2018), προσπαθώντας να ισορροπήσουν τη διαφάνεια και τη λογοδοσία με το απόρρητο (Phillips, 2018). Οι οργανισμοί πρέπει να προσαρμόζονται στις διαφορετικές νομοθετικές απαιτήσεις διεθνώς, εξασφαλίζοντας ότι οι πρακτικές τους προστατεύουν αποτελεσματικά τα δεδομένα προσωπικού χαρακτήρα σύμφωνα με τις αρχές της εκάστοτε νομοθεσίας.

Οι οργανισμοί είναι υποχρεωμένοι να εναρμονίζονται με μια πληθώρα νομοθετικών προτύπων και κανονιστικών πλαισίων προστασίας δεδομένων για να εξασφαλίσουν την προστασία και το απόρρητο των προσωπικών πληροφοριών. Στον Καναδά, οι οργανισμοί υπάγονται στον Νόμο περί Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA), ο οποίος τους καθιστά υπεύθυνους για τις προσωπικές πληροφορίες που διαχειρίζονται ή φυλάσσουν, καθώς και για εκείνες που μεταβιβάζονται σε τρίτους για επεξεργασία (Phillips, 2018). Αυτός ο νόμος βασίζεται στις αρχές που ορίζονται στις Κατευθυντήριες Γραμμές του Οργανισμού για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ) για την προστασία της ιδιωτικότητας (Phillips, 2018).

Στην Ευρωπαϊκή Ένωση, οι οργανισμοί πρέπει να συμμορφώνονται με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), ο οποίος θέτει το πλαίσιο για την προστασία δεδομένων στην ΕΕ. Ο GDPR ορίζει επίσης τις διαδικασίες για τη διεθνή μεταφορά δεδομένων, μέσω του Κεφαλαίου V, απαιτώντας από τους οργανισμούς να ακολουθούν εγκεκριμένους κώδικες δεοντολογίας για την εξασφάλιση αποτελεσματικών διασφαλίσεων κατά τη μεταφορά προσωπικών δεδομένων (Phillips, 2018).

Στις Ηνωμένες Πολιτείες, ο Νόμος Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας του 1996 (HIPAA) ρυθμίζει την προστασία δεδομένων στον τομέα της υγείας, επιβάλλοντας απαιτήσεις για την προστασία υγειονομικών πληροφοριών (Phillips, 2018). Ενώ, η Οδηγία της ΕΕ για την Προστασία Δεδομένων (1995) και ο GDPR (2016) καθορίζουν τις απαιτήσεις για την επεξεργασία και τη μεταφορά προσωπικών δεδομένων εντός και εκτός ΕΕ, με τον GDPR να παρέχει επιπρόσθετες εξαιρέσεις για σκοπούς επιστημονικής έρευνας μέσω του άρθρου 89 (Phillips, 2018).

Για να διασφαλίσουν τη συμμόρφωση με αυτούς τους νόμους και κανονισμούς, οι οργανισμοί μπορούν να εφαρμόσουν εσωτερικές αξιολογήσεις και να ακολουθήσουν εγκεκριμένους μηχανισμούς για τη διαβίβαση δεδομένων, όπως οι αποφάσεις επάρκειας που

εκδίδονται από την Ευρωπαϊκή Επιτροπή. Επιπλέον, η τήρηση των κανόνων δεοντολογίας και η εφαρμογή δεσμευτικών εταιρικών κανόνων μπορεί να ενισχύσει τη συμμόρφωση με τις διατάξεις του GDPR και άλλων σχετικών νόμων προστασίας δεδομένων. Η προσεκτική ανάλυση και η προσαρμογή των πολιτικών και των πρακτικών σύμφωνα με τις απαιτήσεις κάθε νομοθετικού πλαισίου είναι κρίσιμη για την αποφυγή παραβάσεων και την εξασφάλιση της προστασίας των προσωπικών δεδομένων.

Οι νομοθεσίες και οι κανονισμοί σχετικά με την προστασία δεδομένων φέρνουν σημαντικές νομικές συνέπειες για οργανισμούς και ερευνητικές ομάδες. Ένας εξέχων κανονισμός, ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation - GDPR) της Ευρωπαϊκής Ένωσης, επιδιώκει την προστασία των ατόμων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων (Chassang, 2017). Σύμφωνα με τον GDPR, οι οργανισμοί υποχρεούνται να ακολουθούν αυστηρούς κανόνες ενημέρωσης των υπευθύνων και εκτελεστών της επεξεργασίας σε περίπτωση παραβίασης προσωπικών δεδομένων και, υπό ορισμένες συνθήκες, να επικοινωνούν με τα άτομα των οποίων τα δεδομένα έχουν παραβιαστεί. Οι παραβιάσεις μπορεί να προκαλέσουν σοβαρές απώλειες για τα άτομα, ενώ ο GDPR προσφέρει νέες προβλέψεις για την εφαρμογή δικαιωμάτων στην αρχειοθέτηση και την έρευνα, καταργώντας την Οδηγία 95/46/ΕΚ (Chassang, 2017).

Όσον αφορά τις κυρώσεις για τη μη συμμόρφωση, αυτές μπορεί να είναι αυστηρές και να έχουν σημαντικές οικονομικές συνέπειες για τους οργανισμούς. Στην Ευρώπη, ο GDPR καθορίζει σαφείς κατευθυντήριες γραμμές και επιβάλλει πρόστιμα έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών του οργανισμού ή 20 εκατομμυρίων ευρώ, ανάλογα με το ποιο από τα δύο είναι μεγαλύτερο (Gellert, 2018). Αυτό καθιστά αναγκαία την πλήρη κατανόηση και συμμόρφωση με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων για την αποφυγή σημαντικών προστίμων και την προστασία της φήμης του οργανισμού. Επιπλέον, στον Καναδά, ο νόμος περί Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (Personal Information Protection and Electronic Documents Act - PIPEDA) απαιτεί τη συγκατάθεση για τη συλλογή, χρήση, και αποκάλυψη προσωπικών πληροφοριών και την προστασία αυτών των πληροφοριών από απώλεια ή κλοπή, υπογραμμίζοντας τη σημασία της συμμόρφωσης με το PIPEDA και άλλους σχετικούς κανονισμούς για την αποφυγή οικονομικών κυρώσεων (Phillips, 2018).

Οι οργανισμοί μπορούν να μειώσουν τους νομικούς κινδύνους σχετικά με την προστασία δεδομένων μέσω της εφαρμογής Αξιολογήσεων Επιπτώσεων στην Προστασία Δεδομένων

(Data Protection Impact Assessments - DPIAs) (Demetzou, 2019). Αυτές οι αξιολογήσεις, οι οποίες προβλέπονται ως υποχρεωτικές από το άρθρο 35 του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation - GDPR), απαιτούν από τους οργανισμούς να προσδιορίζουν, αξιολογούν, και διαχειρίζονται υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων πριν από την επεξεργασία προσωπικών δεδομένων (Demetzou, 2019).

Η ενσωμάτωση της προστασίας δεδομένων από το στάδιο του σχεδιασμού και ως προεπιλογή (Data Protection by Design and by Default), καθώς και η διορισμός ενός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer - DPO), ενισχύουν περαιτέρω τη δέσμευση των οργανισμών προς την προστασία δεδομένων και τη μείωση νομικών κινδύνων (Demetzou, 2019). Η εκτέλεση των DPIA προσδιορίζεται ως ένα κρίσιμο βήμα προς την ενίσχυση της λογοδοσίας και της ευθύνης των οργανισμών στο πλαίσιο της εφαρμογής του GDPR, διασφαλίζοντας υψηλό επίπεδο προστασίας δεδομένων και μετριάζοντας τους σχετιζόμενους νομικούς κινδύνους (Demetzou, 2019).

5.2 Προκλήσεις στη συμμόρφωση με το GDPR και άλλους κανονισμούς

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation - GDPR) έχει θέσει σειρά προκλήσεων για τους οργανισμούς παγκοσμίως όσον αφορά τη συμμόρφωση, υποχρεώνοντάς τους να αναθεωρήσουν σημαντικά τις πρακτικές προστασίας δεδομένων τους ή να αντιμετωπίσουν σοβαρές κυρώσεις (Tankard, 2016). Η συμμόρφωση με τον GDPR απαιτεί εκτενή χρονική και πρακτική δέσμευση, η οποία διαφέρει ανάλογα με τη δομή και το μέγεθος κάθε οργανισμού. Ειδικά, η δυσκολία προσαρμογής στην ταχεία τεχνολογική εξέλιξη αποτελεί μείζονα πρόκληση, καθώς ο GDPR αποφεύγει την υπερβολικά προσδιοριστική κανονιστική προσέγγιση ώστε να παραμένει επίκαιρος (Tankard, 2016). Αυτό σημαίνει ότι οι οργανισμοί πρέπει να βρουν δικές τους λύσεις στην επίτευξη συμμόρφωσης, χωρίς συγκεκριμένη καθοδήγηση σχετικά με τις τεχνολογίες που θα πρέπει να χρησιμοποιηθούν.

Η ανησυχία για την αντιμετώπιση προστίμων λόγω μη συμμόρφωσης εντείνεται από την πεποίθηση πολλών οργανισμών ότι ο GDPR θα αυξήσει δραματικά το κόστος των επιχειρηματικών δραστηριοτήτων στην Ευρώπη, με κάποιους να προβλέπουν αυξήσεις

προϋπολογισμού έως και 10% για την αντιμετώπιση των απαιτήσεων του GDPR. Επιπρόσθετα, το επίπεδο συμμόρφωσης που απαιτείται από τον GDPR επεκτείνεται σε όλους τους οργανισμούς που διαχειρίζονται δεδομένα πολιτών της ΕΕ, ανεξαρτήτως της γεωγραφικής τους θέσης, εισάγοντας πρόσθετες προκλήσεις για τη συμμόρφωση, ιδίως για εκείνους που εξαρτώνται από υπηρεσίες cloud. Η απαίτηση για σαφή συγκατάθεση, το δικαίωμα αντίρρησης, και το δικαίωμα στη λήθη, καθιστούν τη συμμόρφωση ακόμη πιο απαιτητική, καθώς αυτά τα δικαιώματα διευρύνουν το πεδίο προστασίας δεδομένων και απαιτούν σημαντικές τροποποιήσεις στις υφιστάμενες πολιτικές και διαδικασίες διαχείρισης δεδομένων. Οι οργανισμοί αντιμετωπίζουν την πρόκληση να διασφαλίσουν την προστασία όλων των δεδομένων, δομημένων και μη, σε όλες τις φάσεις της επεξεργασίας και αποθήκευσης, υιοθετώντας την κρυπτογράφηση ως προεπιλεγμένη επιλογή (Tankard, 2016).

Οι οργανισμοί αντιμετωπίζουν σημαντικές προκλήσεις στην προσπάθεια τους να συμμορφωθούν με τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation - GDPR) και άλλους σχετικούς κανονισμούς. Για να ξεπεράσουν αυτές τις προκλήσεις, απαιτείται μια συνεκτική στρατηγική που συνδυάζει επιμελή προσέγγιση και συνεργασία εντός του οργανισμού. Η υιοθέτηση συστημάτων διαχείρισης συμμόρφωσης προσφέρει έναν αποτελεσματικό τρόπο για την παρακολούθηση και τη διαχείριση των κινδύνων, ενώ η χρήση εργαλείων για την παρακολούθηση και τον μετριασμό των κινδύνων συμβάλλει στην αποτελεσματική εφαρμογή των απαιτήσεων συμμόρφωσης στις επιχειρηματικές μονάδες (Kulkarni et al., 2021; Augustine, 2019).

Επιπλέον, η αναζήτηση συμβουλών από ειδικούς στον τομέα της συμμόρφωσης και η ανταλλαγή πληροφοριών με ομοτίμους του κλάδου μπορούν να προσφέρουν πολύτιμη καθοδήγηση και να συμβάλλουν στην αποτελεσματική προσαρμογή στις απαιτήσεις του GDPR (Augustine, 2019). Οι μικρές και μεσαίες επιχειρήσεις (ΜΜΕ) έχουν τη δυνατότητα να υπερβούν τους περιορισμούς πόρων μέσω της ανάθεσης εργασιών συμμόρφωσης σε τρίτους παρόχους ή επενδύοντας στην εκπαίδευση και ανάπτυξη των εργαζομένων τους (Augustine, 2019).

Η ιεράρχηση των προτεραιοτήτων καιη υιοθέτηση τεχνολογίας για την αυτοματοποίηση των διαδικασιών συμμόρφωσης μπορούν επίσης να συμβάλλουν σημαντικά στην αποτελεσματική διαχείριση και εκπλήρωση των κανονιστικών απαιτήσεων (Augustine, 2019). Η απλοποίηση της γλώσσας των κανονισμών και η επένδυση σε προγράμματα

κατάρτισης για τους εργαζομένους μπορούν να βοηθήσουν στην καλύτερη κατανόηση και εφαρμογή των απαιτήσεων συμμόρφωσης (Kulkarni et al., 2021).

Η κατανόηση των κανονιστικών απαιτήσεων και των επιπτώσεων τους στην επιχείρηση αποτελεί θεμελιώδες βήμα για την αντιμετώπιση των προκλήσεων συμμόρφωσης. Τέλος, η εναρμόνιση της διασυνοριακής συμμόρφωσης μπορεί να βοηθήσει τους οργανισμούς να αποφύγουν πρόστιμα, νομικές διαφορές, και ζημιά στη φήμη, διασφαλίζοντας ταυτόχρονα την ακεραιότητα και τη σταθερότητα των ιδρυμάτων τους (Augustine, 2019). Η υιοθέτηση λειτουργικών μεθοδολογιών και τεχνολογίας για την αξιοποίηση της ανθρώπινης τεχνογνωσίας και τη λειτουργία σε κλίμακα είναι κρίσιμη για την επιτυχή αντιμετώπιση των προκλήσεων συμμόρφωσης (Aslam et al., 2023).

Η εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) παρουσιάζει σημαντικές προκλήσεις για τους οργανισμούς παγκοσμίως, αναγκάζοντάς τους να προσαρμοστούν σε ένα νέο κανονιστικό πλαίσιο ή να αντιμετωπίσουν σοβαρές κυρώσεις (Tankard, 2016). Οι προκλήσεις στην επίτευξη συμμόρφωσης είναι πολυδιάστατες και συχνά εξαρτώνται από τη φύση, το μέγεθος και τη γεωγραφική κατανομή του οργανισμού, καθώς και από τον τύπο των δεδομένων που επεξεργάζεται.

Μία σημαντική πρόκληση είναι η δυσκολία στην προσαρμογή στις ταχύτατες τεχνολογικές εξελίξεις, καθώς ο GDPR απαιτεί από τους οργανισμούς να εφαρμόζουν τεχνολογίες και διαδικασίες που διασφαλίζουν την προστασία των δεδομένων (Tankard, 2016). Επιπλέον, ο κανονισμός δεν ορίζει συγκεκριμένες τεχνολογίες για την επίτευξη συμμόρφωσης, αφήνοντας τους οργανισμούς να ερμηνεύσουν και να επιλέξουν τις κατάλληλες λύσεις. Αυτό δημιουργεί αβεβαιότητα και απαιτεί αυξημένη προσπάθεια και εμπειρογνωμοσύνη για την εξασφάλιση της συμμόρφωσης.

Η ανησυχία για πιθανά πρόστιμα αποτελεί μια άλλη σημαντική πρόκληση. Ο GDPR προβλέπει αυστηρές οικονομικές κυρώσεις για παραβιάσεις, με πρόστιμα που μπορεί να φτάσουν έως και το 4% του ετήσιου παγκόσμιου κύκλου εργασιών ή 20 εκατομμύρια ευρώ, ανάλογα με το ποιο είναι υψηλότερο (Gellert, 2018). Αυτή η προοπτική προκαλεί ανησυχία στους οργανισμούς και τους ωθεί στη λήψη ενεργειών για την αποφυγή τέτοιων κυρώσεων, προσθέτοντας περισσότερο κόστος και περιορισμούς στις επιχειρηματικές τους δραστηριότητες.

Επιπρόσθετα, η εφαρμογή του GDPR απαιτεί από τους οργανισμούς να προβούν σε σημαντικές αλλαγές στις πολιτικές απορρήτου και τις διαδικασίες επεξεργασίας δεδομένων, κάτι που μπορεί να είναι ιδιαίτερα προκλητικό για μικρότερους οργανισμούς ή εκείνους με περιορισμένους πόρους (Mohan et al., 2019). Η ανάγκη για διαφάνεια και λεπτομερής καταγραφή των διαδικασιών επεξεργασίας δεδομένων αυξάνει την πολυπλοκότητα και το κόστος της συμμόρφωσης.

Για να αντιμετωπίσουν αυτές τις προκλήσεις, οι οργανισμοί πρέπει να υιοθετήσουν ένα συνεκτικό πλαίσιο για τη συμμόρφωση με τον GDPR, το οποίο περιλαμβάνει την υιοθέτηση βέλτιστων πρακτικών όπως η διαφάνεια, η ακρίβεια, η ελαχιστοποίηση δεδομένων, ο περιορισμός σκοπού και η λογοδοσία (Mohan et al., 2019). Επιπλέον, η ενίσχυση των τεχνολογικών δυνατοτήτων και η συνεχής εκπαίδευση των εργαζομένων σε θέματα προστασίας δεδομένων είναι κρίσιμης σημασίας για την προώθηση της συμμόρφωσης και την αποφυγή πιθανών προστίμων.

Η διασφάλιση συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων αποτελεί μια εκ των προτέρων δαπανηρή διαδικασία για τις οργανώσεις, κυρίως για τις Μικρομεσαίες Επιχειρήσεις (ΜΜΕ), όπως αναφέρεται από τους Li et al. (2022). Ενώ οι μεγάλες επιχειρήσεις μπορεί να επιβαρύνονται λιγότερο από το κόστος συμμόρφωσης, οι ΜΜΕ με περιορισμένους πόρους μπορεί να βρουν προκλητική την κατεύθυνση των περιορισμένων οικονομικών τους προς τη συμμόρφωση και την ανάπτυξη (Li et al., 2022). Η προσλήψη ειδικών ομάδων νομικών και εμπειρογνωμόνων σε θέματα ιδιωτικότητας είναι μία από τις προσεγγίσεις για τη διασφάλιση συμμόρφωσης, αλλά αυτό μπορεί να μην είναι πρακτικό για τις ΜΜΕ λόγω του υψηλού κόστους που συνεπάγεται (Li et al., 2022).

Επιπροσθέτως, οι οργανώσεις αντιμετωπίζουν προκλήσεις στη συμμόρφωση με συγκεκριμένες υποχρεώσεις υπό το πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), όπως την ειδοποίηση ατόμων σε περίπτωση παραβίασης δεδομένων και την τεκμηρίωση δραστηριοτήτων επεξεργασίας δεδομένων, οι οποίες μπορεί να αποτελέσουν σημαντικές προκλήσεις για τις οργανώσεις (Chhetri et al., 2022). Η παροχή πληροφοριών και αποκαλύψεων σχετικά με την επεξεργασία δεδομένων στα άτομα αποτελεί επίσης μια δύσκολη διαδικασία για τις οργανώσεις να διαχειριστούν (Chhetri et al., 2022).

Για την αντιμετώπιση αυτών των προκλήσεων, απαιτείται μια ενδελεχής, στρατηγική προσέγγιση και η συνεργασία μεταξύ διαφορετικών τμημάτων της οργάνωσης. Η εφαρμογή συστημάτων διαχείρισης συμμόρφωσης που βοηθούν στην παρακολούθηση κινδύνων και

τον έλεγχο των μέτρων μετριασμού μπορεί να συνεισφέρει στην υπέρβαση των προκλήσεων (Kulkarni et al., 2021; Augustine, 2019).

Η εναρμόνιση της διασυνοριακής συμμόρφωσης και η υιοθέτηση τεχνολογιών για την αυτοματοποίηση των διαδικασιών συμμόρφωσης μπορεί επίσης να βοηθήσει τις οργανώσεις να αντιμετωπίσουν αποτελεσματικά τις προκλήσεις (Augustine, 2019). Η συνεργασία δημόσιου και ιδιωτικού τομέα είναι ζωτικής σημασίας για την ενίσχυση της κατανόησης και της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων, καθώς και για την αποφυγή σημαντικών προστίμων, νομικών διαφορών και ζημιάς στη φήμη (Gurkaynak et al., 2014).

Η συμμόρφωση με τις αυξανόμενες απαιτήσεις των κανονισμών προστασίας δεδομένων αποτελεί σημαντική πρόκληση για οργανισμούς παγκοσμίως, απαιτώντας ενίσχυση των μηχανισμών απορρήτου και συμμόρφωσης. Ειδικά, ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης αποτελεί παράδειγμα ενός ολοκληρωμένου κανονισμού που καλύπτει διάφορες πτυχές της προστασίας προσωπικών δεδομένων, συμπεριλαμβανομένων των δικαιωμάτων διαγραφής και προστασίας από αυτοματοποιημένες αποφάσεις (Li et al., 2021). Η ανωνυμοποίηση δεδομένων εμφανίζεται ως βιώσιμη στρατηγική για την εκπλήρωση των απαιτήσεων των κανονισμών, με τα ανώνυμα δεδομένα να εξαιρούνται συνήθως από τους κανονισμούς προστασίας προσωπικών δεδομένων, διατηρώντας ταυτόχρονα την πληροφοριακή τους αξία (Li et al., 2021). Η επιλογή των αναγνωριστικών αποτελεί κρίσιμη διαδικασία για την πρόληψη επιθέσεων σύνδεσης δεδομένων, με την ανάγκη για αφαίρεση ή ανωνυμοποίηση άμεσων και έμμεσων αναγνωριστικών πριν από τη δημοσίευση συνόλων δεδομένων (Li et al., 2021).

Επιπλέον, η τέλεια ανωνυμοποίηση μπορεί να μην είναι πάντα εφικτή, συνεπώς η εστίαση θα πρέπει να είναι στη μείωση του κινδύνου επαναπροσδιορισμού μέσω της μετατροπής των δεδομένων σε μορφή όπου ο κίνδυνος ελαχιστοποιείται (Li et al., 2021). Οι αυστηρότεροι κανονισμοί προστασίας προσωπικών δεδομένων που έχουν εφαρμοστεί παγκοσμίως έχουν ως στόχο την πρόληψη περιστατικών παράνομης χρήσης, ακατάλληλης χρήσης δεδομένων πελατών, και συχνών διαρροών δεδομένων, παρέχοντας προκλήσεις ιδιαίτερα για τις μικρές και μεσαίες επιχειρήσεις (ΜΜΕ) στην προσπάθειά τους να δημιουργήσουν συνέργεια από τις προσπάθειες συλλογής δεδομένων (Li et al., 2021). Οι ιδιωτικοί οργανισμοί θα πρέπει να απέχουν από την κοινή χρήση ή δημιουργία συνόλων δεδομένων που παραβιάζουν τους κανονισμούς περί απορρήτου, εστιάζοντας στην πρόληψη της σύνδεσης δεδομένων μέσω της κατάλληλης επεξεργασίας άμεσων και έμμεσων αναγνωριστικών (Li et al., 2021).

Κεφάλαιο 6ο: Μεθοδολογία

6.1 Σκοπός και ερευνητικά ερωτήματα

Σκοπός της έρευνας αυτής είναι να διερευνήσει το βαθμό συμμόρφωσης των επιχειρήσεων με το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων.

Τα ερευνητικά ερωτήματα είναι τα εξής:

- Σε ποιο βαθμό οι επιχειρηματίες γνωρίζουν το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων;
- Σε ποιο βαθμό οι επιχειρήσεις συμμορφώνονται με το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων;
- Ποιες είναι οι αντιλήψεις των επιχειρηματιών για το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων;
- Υπάρχουν διαφοροποιήσεις στο βαθμό συμμόρφωσης και τις αντιλήψεις για το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων ανάλογα τα δημογραφικά στοιχεία των επιχειρηματιών και τα στοιχεία των επιχειρήσεων;

6.2 Δείγμα

Το δείγμα της έρευνας ήταν 70 επιχειρηματίες. Πραγματοποιήθηκε δειγματοληψία ευκολίας. Η δειγματοληψία ευκολίας είναι μια μη πιθανοτική μέθοδος δειγματοληψίας, όπου επιλέγονται άτομα για συμπερίληψη στο δείγμα εκείνα για τα οποία έχει την ευκολότερη πρόσβαση ο ερευνητής. Επιλέχθηκε λοιπόν αυτή η μέθοδος δειγματοληψίας γιατί εξασφαλίζει εύκολη και γρήγορη συλλογή δείγματος (Δαφέρμος, 2011).

6.3 Μέθοδος συλλογής δεδομένων

Η παρούσα έρευνα είναι ποσοτική συγχρονική. Δημιουργήθηκε ένα αυτοσχέδιο

ερωτηματολόγιο για να συλλεχθούν τα δεδομένα. Επιλέχθηκε ποσοτική έρευνα καθώς εξασφαλίζει την εύκολη και γρήγορη συλλογή δεδομένων από μεγάλο δείγμα ατόμων ενώ παράλληλα εξασφαλίζεται η ανωνυμία των συμμετεχόντων (Δαφέρμος, 2011).

Αναλυτικότερα, δημιουργήθηκε ένα ερωτηματολόγιο το οποίο αποτελούνταν από 24 ερωτήσεις. Το ερωτηματολόγιο βασίστηκε στην υπάρχουσα βιβλιογραφία σχετικά με το θέμα, και διαμορφώθηκε με βάση τις ανάγκες της παρούσας έρευνας. Χρησιμοποιήθηκαν 19 ερωτήσεις κλειστού τύπου και 5 ερωτήσεις σε μια πενταβάθμια κλίμακα Likert (βλ. Παράρτημα).

Το ερωτηματολόγιο της έρευνας είχε πέντε θεματικές: α) δημογραφικά χαρακτηριστικά και στοιχεία επιχείρησης (7 ερωτήσεις), β) γνώση και συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (13 ερωτήσεις), γ) αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων (4 ερωτήσεις) (βλ. Παράρτημα).

Αναφορικά με τα δημογραφικά χαρακτηριστικά των συμμετεχόντων μελετήθηκε το φύλο, η ηλικία, το μορφωτικό επίπεδο και η θέση στην επιχείρηση. Όσον αφορά τα στοιχεία της επιχείρησης, εξετάστηκε το είδος της, το μέγεθός της και ο τομέας δραστηριοποίησής της.

Για τη δεύτερη θεματική, εξετάστηκε ο βαθμός που οι συμμετέχοντες γνώριζαν τον Γενικό Κανονισμό για την Προστασία των Δεδομένων. Μελετήθηκε επίσης εάν έχει γίνει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων, αν διατηρούνται τα προσωπικά δεδομένα πελατών, συνεργατών, προμηθευτών και υπαλλήλων (δηλ. ονοματεπώνυμο, διεύθυνση, κινητό τηλέφωνο, email κλπ), αν διαμοιράζονται τα προσωπικά δεδομένα που διατηρούνται με άλλους οργανισμούς και επιχειρήσεις, και αν γίνεται χρήση των προσωπικών δεδομένων που διατηρούνται για προωθητικές ενέργειες πωλήσεων. Εξετάστηκε επίσης εάν όταν αποστέλλονται email ή SMS στα άτομα των οποίων διατηρούνται τα προσωπικά τους δεδομένα, δίνεται η δυνατότητα διακοπής της επικοινωνίας (διαγραφή) με κατανοητό και απλό τρόπο. Οι συμμετέχοντες ρωτήθηκε επίσης εάν τα φυσικά πρόσωπα γνωρίζουν ότι έχουν τα προσωπικά τους δεδομένα και τον λόγο και τον τρόπο χρήσης τους, εάν τα προσωπικά δεδομένα διατηρούνται για όσο διάστημα χρειάζεται, εάν διατηρούνται ακριβή και ενημερωμένα, και ασφαλή. Οι εργαζόμενοι ερωτήθηκαν επιπλέον εάν γνώριζαν τα δικαιώματα των ατόμων των οποίων

διατηρούν και αποθηκεύουν τα προσωπικά τους δεδομένα, καθώς και ποια δικαιώματα μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούν και αποθηκεύουν τα προσωπικά τους δεδομένα. Τέλος, οι εργαζόμενοι ερωτήθηκαν εάν στην ιστοσελίδα της επιχείρησης περιγράφεται λεπτομερώς η πολική απορρήτου προσωπικών δεδομένων της επιχείρησης.

Όσον αφορά την τρίτη θεματική του ερωτηματολογίου, εξετάστηκε ο βαθμός στον οποίο οι συμμετέχοντες θεωρούσαν εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ο βαθμός στον οποίο θεωρούσαν δύσκολη την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, καθώς και ο βαθμός στον οποίο θεωρούσαν ότι το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων είναι υψηλό. Εξετάστηκε επίσης ο βαθμός στον οποίο οι εργαζόμενοι πίστευαν ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης.

6.4 Διαδικασία

Το ερωτηματολόγιο διανεμήθηκε και απαντήθηκε μέσω Google Forms κατά την περίοδο Οκτώβριος-Δεκέμβριος 2023. Οι συμμετέχοντες ήταν γνώστες του σκοπού της έρευνας και του γεγονότος ότι η έρευνα διεξάγεται στα πλαίσια μεταπτυχιακών σπουδών. Γνώριζαν επίσης το σκοπό της μελέτης. Η ανωνυμία των συμμετεχόντων εξασφαλίστηκε και οι απαντήσεις ήταν εμπιστευτικές. Πρόσβαση στις απαντήσεις είχε μόνο ο ερευνητής. Επίσης, δόθηκαν στοιχεία επικοινωνίας (email) σε περίπτωση απορίων ή διευκρινήσεων. Η συμμετοχή στην έρευνα ήταν εθελοντική, και διευκρινίστηκε στους συμμετέχοντες ότι οι απαντήσεις τους θα διατηρηθούν για ένα χρόνο και έπειτα θα γίνει οριστική διαγραφή τους.

6.5 Στατιστική ανάλυση

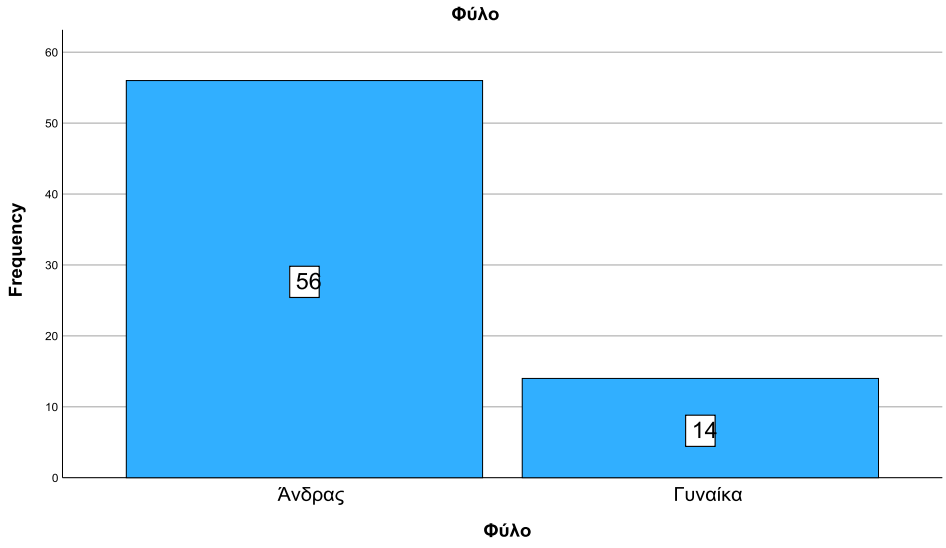
Η στατιστική ανάλυση των δεδομένων έγινε με το λογισμικό IBM SPSS στην έκδοση 29. Πρώτα από όλα, πραγματοποιήθηκε η κατάλληλη κωδικοποίηση των δεδομένων και χρησιμοποιήθηκε περιγραφική στατιστική για την παρουσίαση των απαντήσεων των συμμετεχόντων. Επίσης, χρησιμοποιήθηκε επαγωγική στατιστική. Μετά από έλεγχο

κατανομής με Kolmogorov-Smirnov βρέθηκε ότι η κατανομή δεν ήταν κανονική (sig < 0,05), οπότε χρησιμοποιήθηκαν μη παραμετρικά τεστ. Συγκεκριμένα πραγματοποιήθηκαν Mann-Whitney tests και Kruskal-Wallis tests, καθώς και chi-square tests.

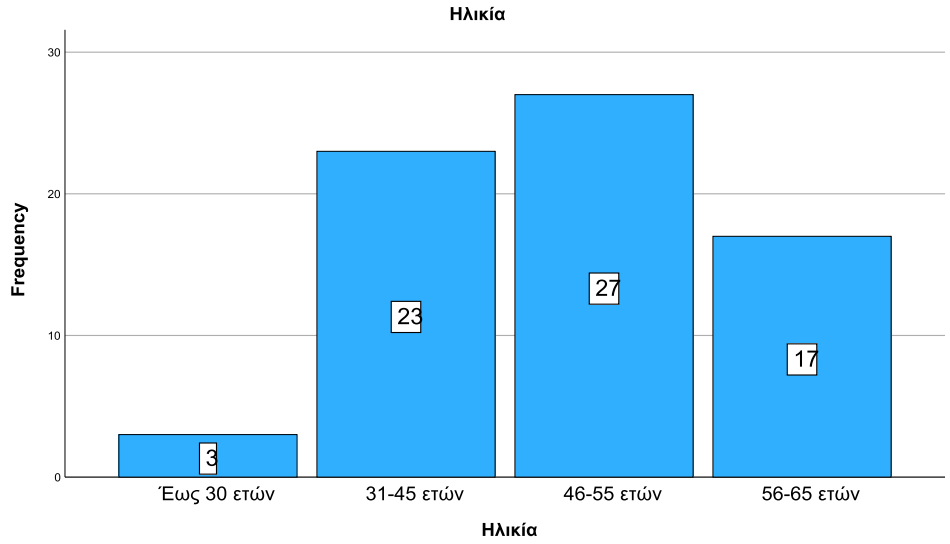
Κεφάλαιο 7ο: Αποτελέσματα

7.1 Περιγραφική στατιστική

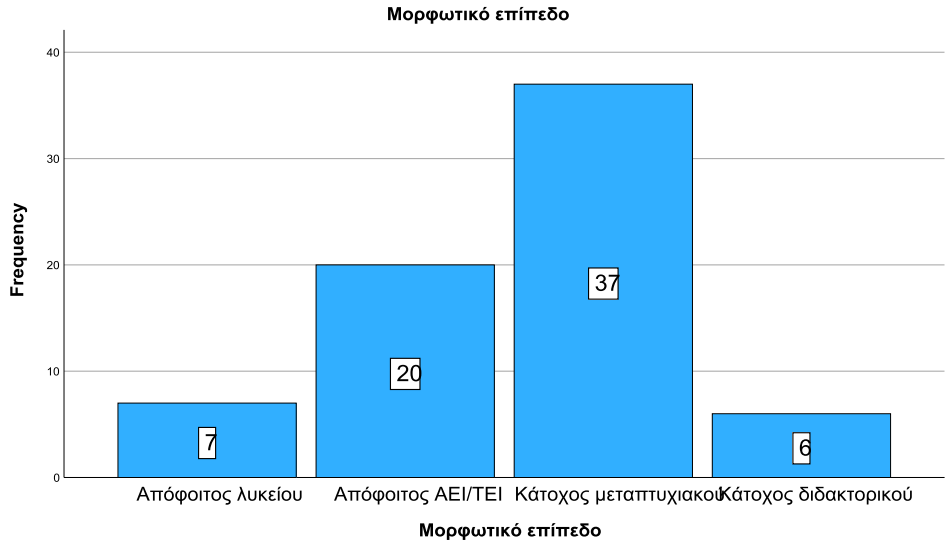
Το δείγμα της έρευνας αποτελούνταν από 56 άνδρες (80%) και 14 γυναίκες (20%) (Διάγραμμα 1). Το 4,3% (n=3) ήταν έως 30 ετών, ενώ το 32,9% (n=23) ήταν 31-45 ετών, το 38,6% (n=27) ήταν 46-55 ετών και το 24,3% (n=17) ήταν 56-65 ετών (Διάγραμμα 2). Το 10% (n=7) ήταν απόφοιτοι λυκείου, το 28,6% (n=20) ήταν απόφοιτοι ΑΕΙ/ΤΕΙ, ενώ το 52,9% (n=37) ήταν κάτοχοι μεταπτυχιακού και το 8,6% (n=6) ήταν κάτοχοι διδακτορικού (Διάγραμμα 3). Επιπλέον, αναφορικά με τη θέση στην επιχείρηση, το 11,4% (n=8) ήταν ιδιοκτήτες, το 30% (n=21) διευθυντές, το 35,7% (n=25) στελέχη και το 22,9% (n=16) μέτοχοι (Διάγραμμα 4).



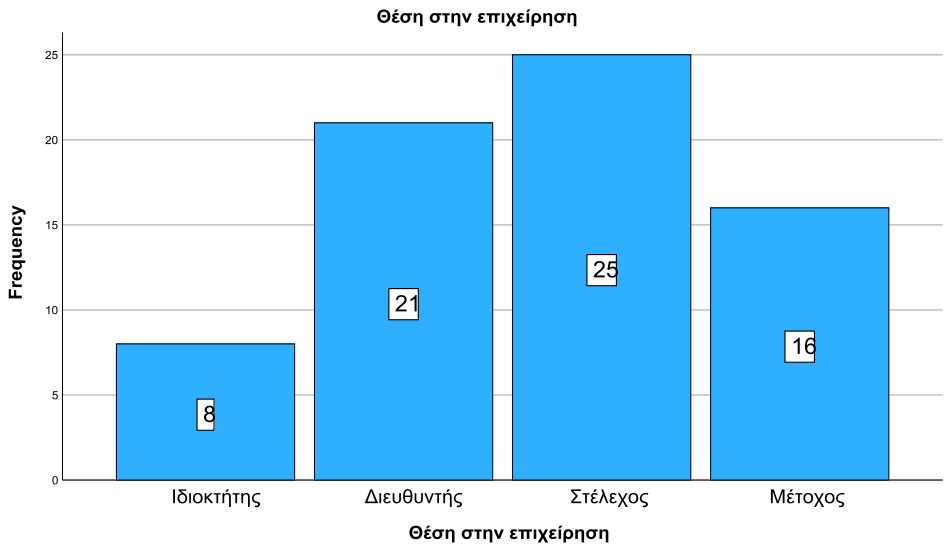
Διάγραμμα 1. Φύλο



Διάγραμμα 2. Ηλικία

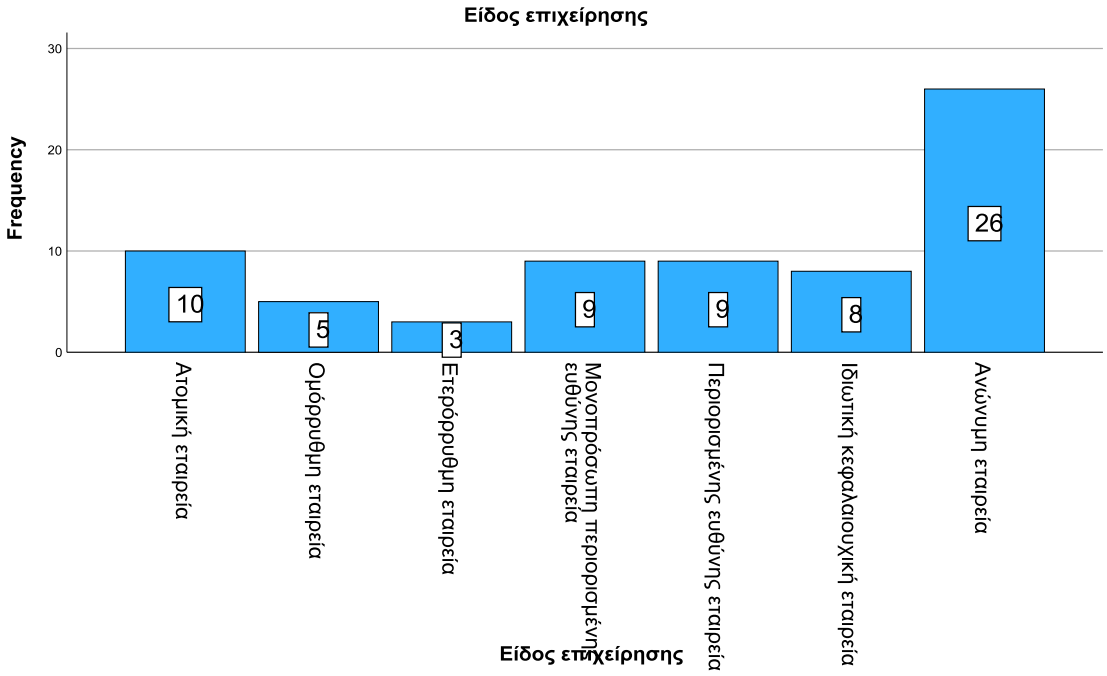


Διάγραμμα 3. Μορφωτικό επίπεδο

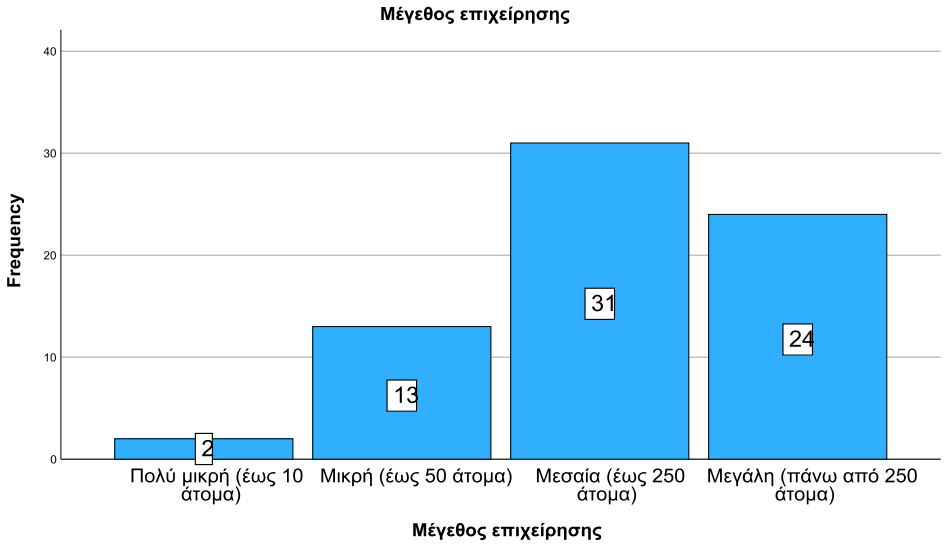


Διάγραμμα 4. Θέση στην επιχείρηση

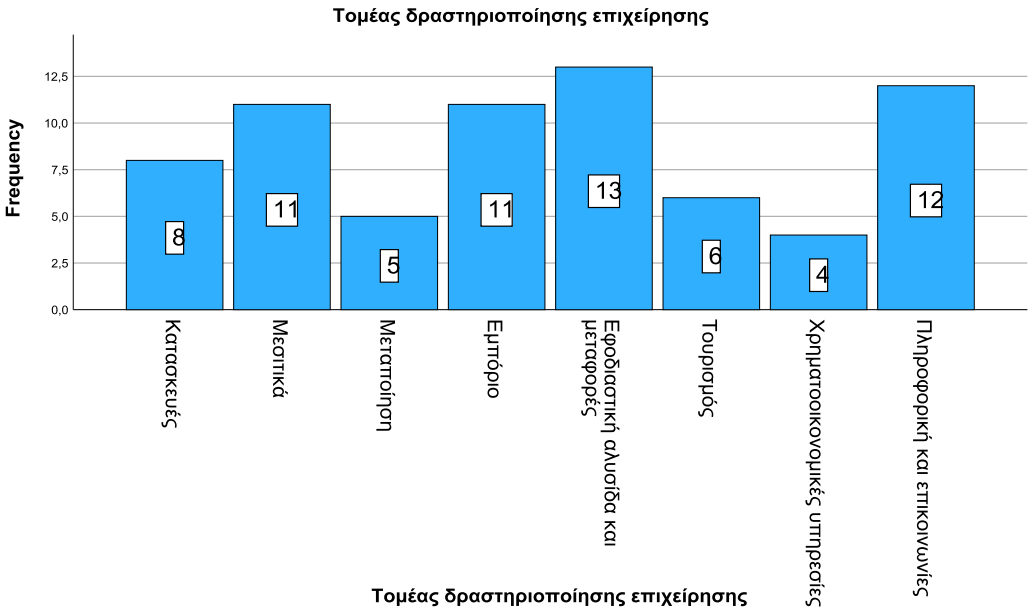
Παράλληλα, όσον αφορά την επιχείρηση, το 14,3% (n=10) ήταν ατομικές εταιρείες, το 7,1% (n=5) ομόρρυθμες εταιρείες, το 4,3% (n=4) ετερόρρυθμες, το 12,9% (n=9) μονοπρόσωπες περιορισμένης ευθύνης, το 12,9% (n=9) περιορισμένης ευθύνης, το 11,4% (n=8) ιδιωτικές κεφαλαιουχικές, και το 37,1% (n=26) ήταν ανώνυμες εταιρείες (Διάγραμμα 5). Επίσης, το 2,9% (n=2) ήταν πολύ μικρές επιχειρήσεις, ενώ το 18,6% (n=13) ήταν μικρές, το 44,3% (n=31) μεσαίες και το 34,3% (n=24) μεγάλες (Διάγραμμα 6). Όσον αφορά τον τομέα δραστηριοποίησης της επιχείρησης, το 11,4% (n=8) δραστηριοποιούνταν στις κατασκευές, το 15,7% (n=11) στα μεσιτικά, το 7,1% (n=5) στη μεταποίηση, το 15,7% (n=11) στο εμπόριο, το 18,6% (n=13) στην εφοδιαστική αλυσίδα και τις μεταφορές, το 8,6% (n=6) στον τουρισμό, το 5,7% (n=4) στις χρηματοοικονομικές υπηρεσίες και το 17,1% (n=12) στην πληροφορική και τις επικοινωνίες (Διάγραμμα 7).



Διάγραμμα 5. Είδος επιχείρησης

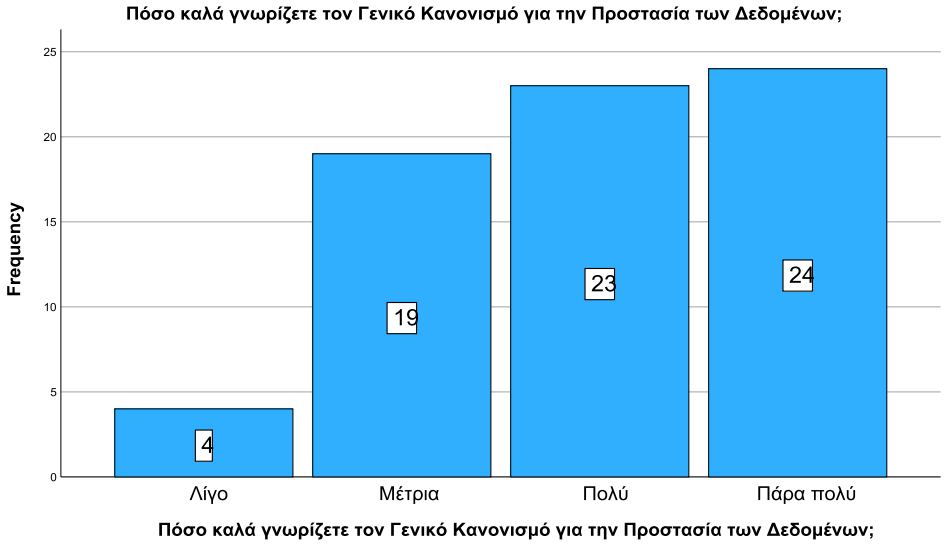


Διάγραμμα 6. Μέγεθος επιχείρησης



Διάγραμμα 7. Τομέας δραστηριοποίησης επιχείρησης

Το 5,7% (n=4) γνώριζαν λίγο τον Γενικό Κανονισμό για την Προστασία των Δεδομένων. Το 27,1% (n=19) τον γνώριζαν μέτρια, το 32,9% (n=23) πολύ και το 34,3% (n=24) πάρα πολύ (Διάγραμμα 8). Παρατηρείται λοιπόν συνολικά ότι οι συμμετέχοντες γνώριζαν ικανοποιητικά το Γενικό Κανονισμό για την Προστασία των Δεδομένων (M= 3.96, SD= .924) (Πίνακας 1).

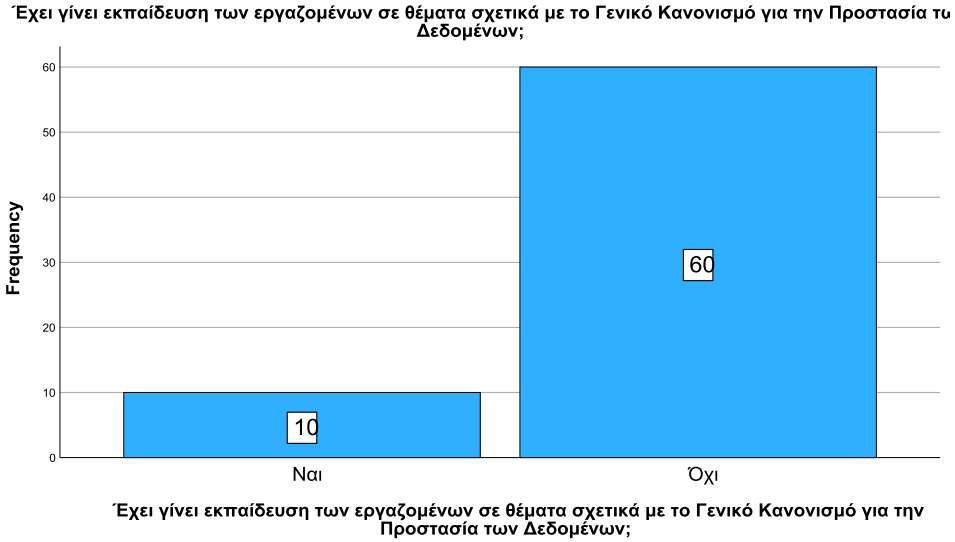


Διάγραμμα 8. Γνώση του Γενικού Κανονισμού για την Προστασία των Δεδομένων

Πίνακας 1. Μέση τιμή και τυπική απόκλιση της γνώσης για το Γενικό Κανονισμό για την Προστασία των Δεδομένων

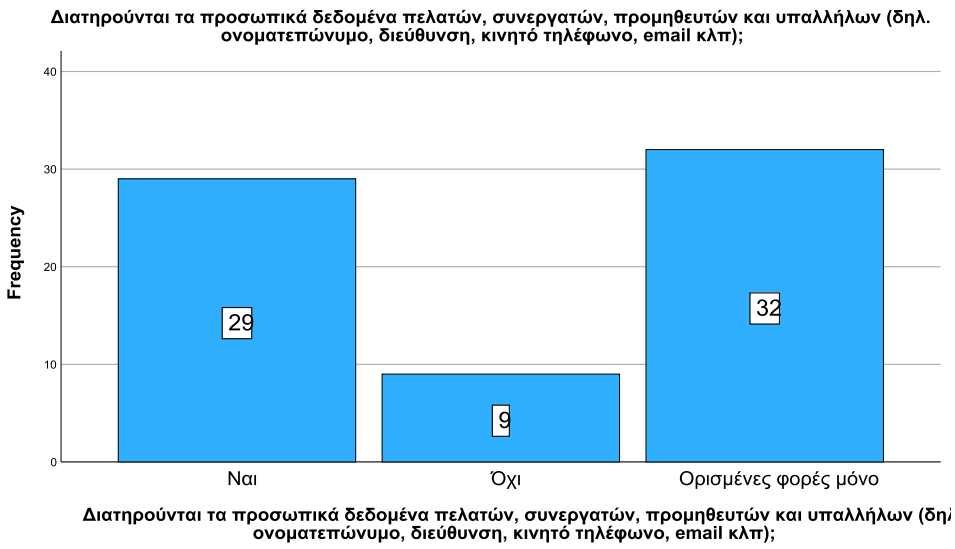
	Μέση τιμή	Τυπική απόκλιση
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	3,96	,924

Επιπρόσθετα, μόνο το 14,3% των συμμετεχόντων (n=10) δήλωσαν πώς είχε γίνει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων (Διάγραμμα 9).

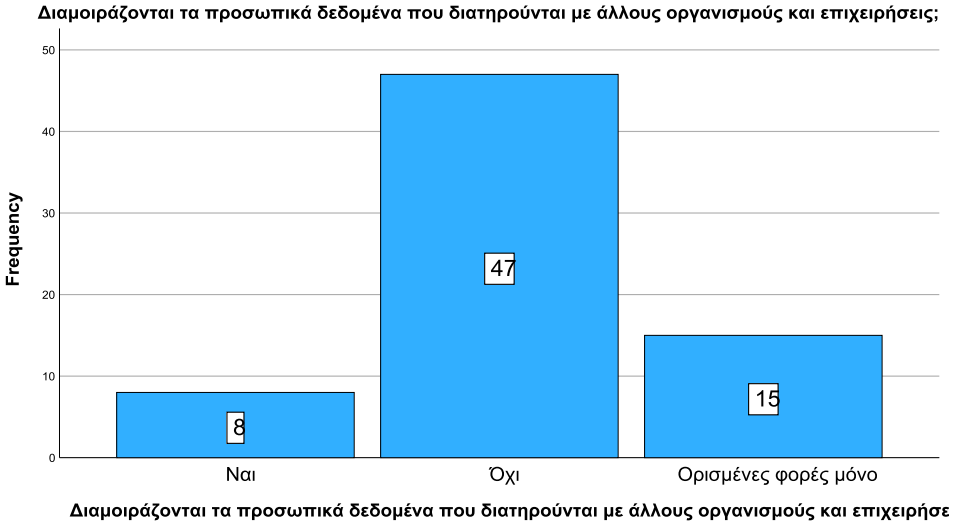


Διάγραμμα 9. Εκπαίδευση εργαζομένων σε θέματα που αφορούν το Γενικό Κανονισμό για την Προστασία των Δεδομένων

Το 41,4% (n=29) δήλωσαν πως διατηρούνταν τα προσωπικά δεδομένα πελατών, συνεργατών, προμηθευτών και υπαλλήλων. Το 12,9% (n=9) δήλωσαν πως δεν διατηρούνταν, ενώ το 45,7% (n=32) δήλωσαν πως διατηρούνταν μόνο ορισμένες φορές (Διάγραμμα 10). Από την άλλη, το 67,1% (n=47) ανέφεραν πως δεν διαμοιράζονταν τα προσωπικά δεδομένα που διατηρούνταν με άλλους οργανισμούς και επιχειρήσεις. Το 11,4% (n=8) ανέφεραν ότι διαμοιράζονται και το 21,4% (n=15) δήλωσαν πως διαμοιράζονταν ορισμένες μόνο φορές (Διάγραμμα 11).



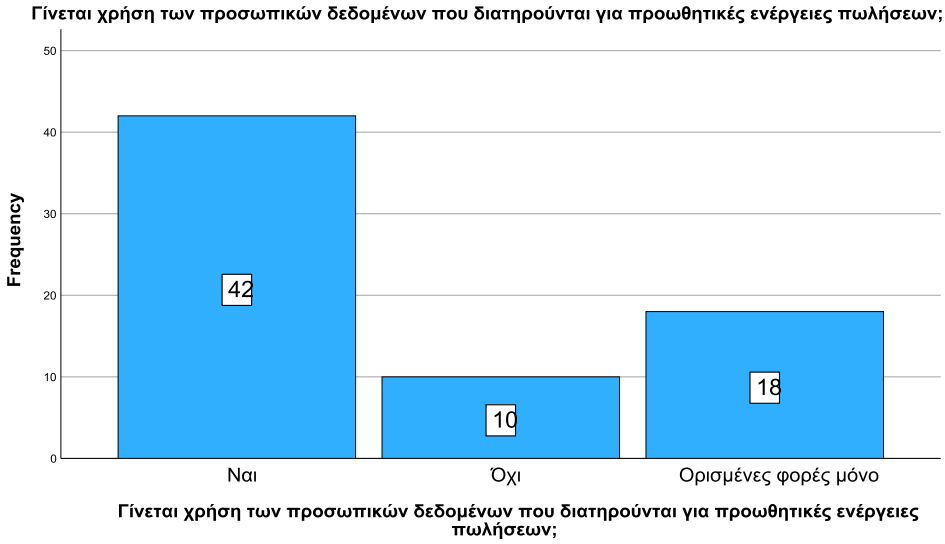
Διάγραμμα 10. Διατήρηση προσωπικών δεδομένων



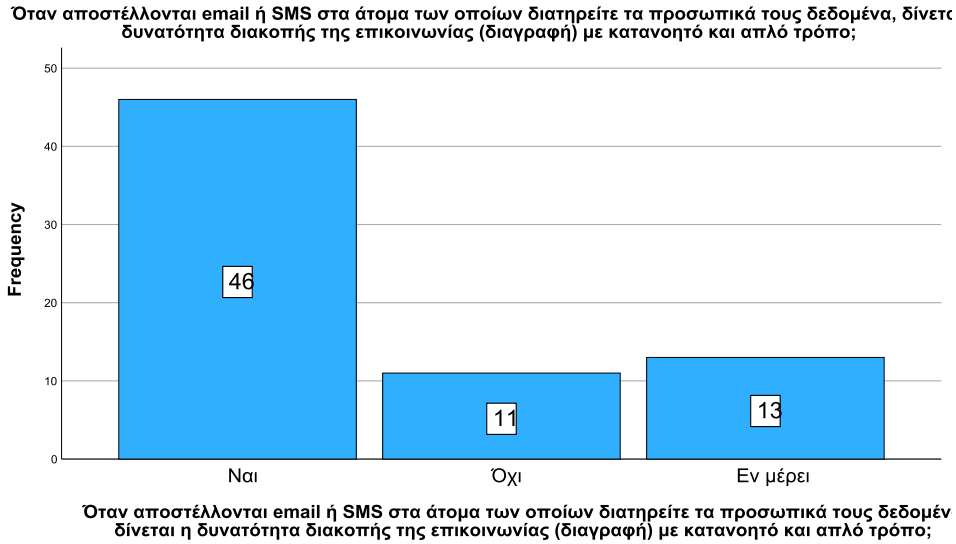
Διάγραμμα 11. Διαμοιρασμός προσωπικών δεδομένων

Ακόμη, το 60% (n=42) δήλωσαν πως γινόταν χρήση των προσωπικών δεδομένων που διατηρούνταν για προωθητικές ενέργειες πωλήσεων. Το 14,3% (n=10) δήλωσαν πως δεν γινόταν χρήση, ενώ το 25,7% (n=18) δήλωσαν πως αυτό συνέβαινε ορισμένες μόνο φορές (Διάγραμμα 12). Ταυτόχρονα, το 65,7% (n=46) δήλωσαν πως όταν αποστέλλονταν email ή SMS στα άτομα των οποίων διατηρούνταν τα προσωπικά τους δεδομένα, δινόταν η δυνατότητα διακοπής της επικοινωνίας (διαγραφή) με κατανοητό και απλό τρόπο. Το 15,7%

(n=11) δήλωσαν πως αυτό δεν γίνονταν, ενώ το 18,6% (n=13) δήλωσαν πως αυτό γίνονταν ορισμένες μόνο φορές (Διάγραμμα 13).

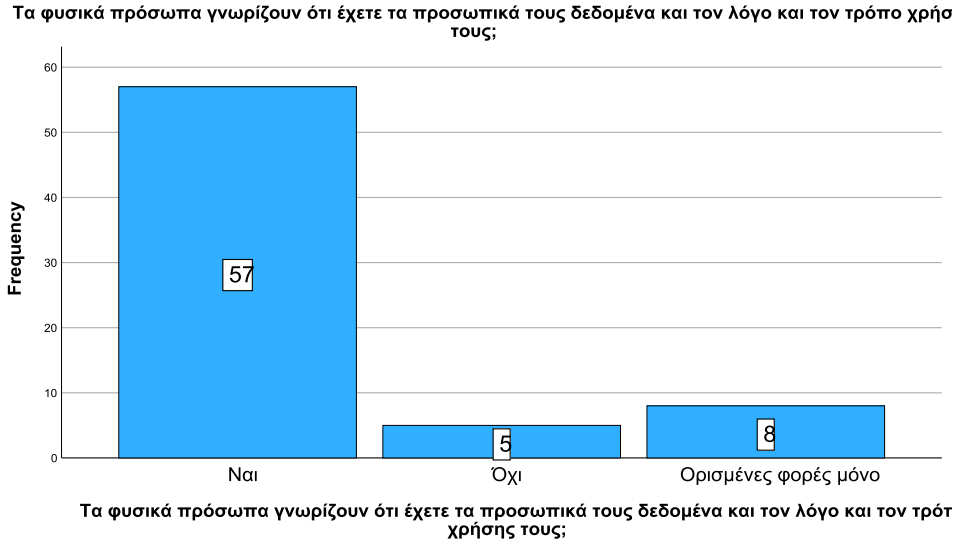


Διάγραμμα 12. Χρήση προσωπικών δεδομένων για προωθητικές ενέργειες πωλήσεων

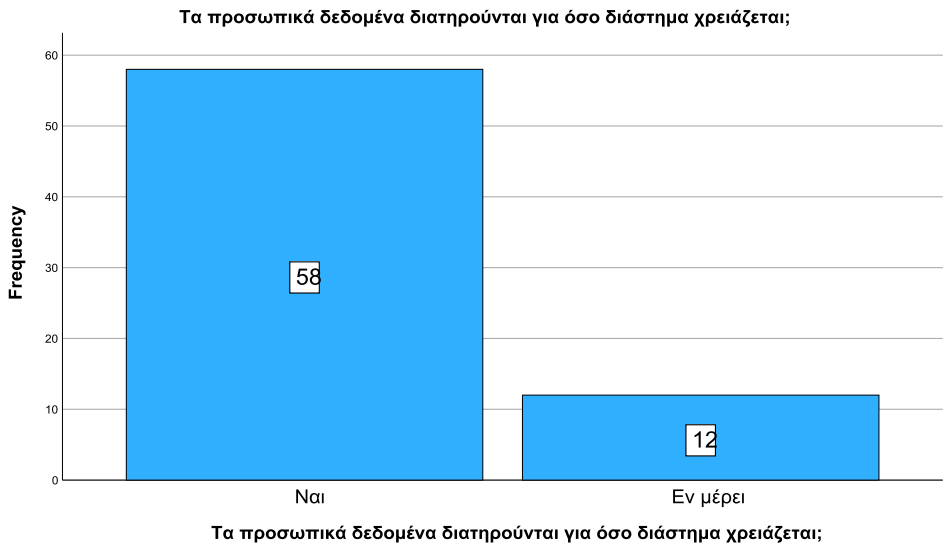


Διάγραμμα 13. Κατανοητός και απλός τρόπος της δυνατότητας διαγραφής

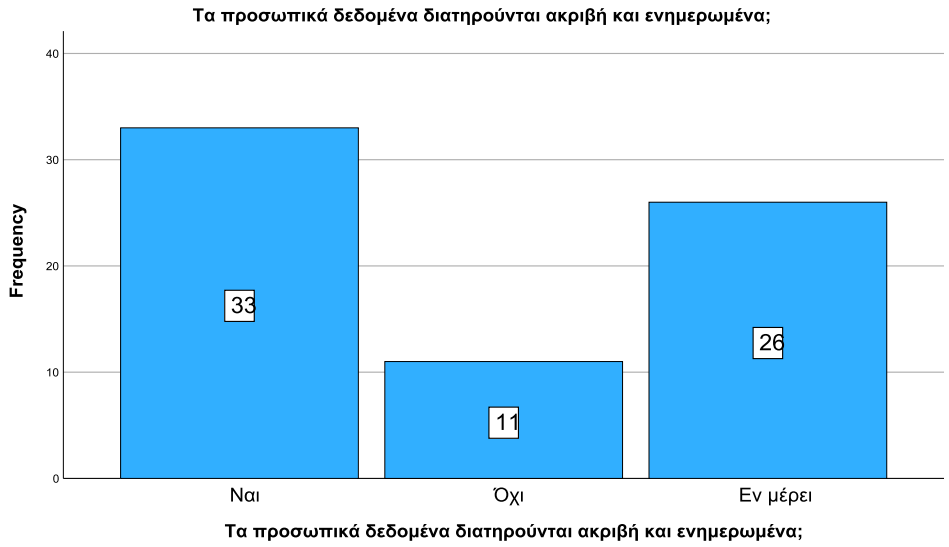
Συνεχίζοντας, το 81,4% (n=57) υποστήριξαν ότι τα φυσικά πρόσωπα γνώριζαν ότι είχαν τα προσωπικά τους δεδομένα και τον λόγο και τον τρόπο χρήσης τους (Διάγραμμα 14), και το 82,9% (n=58) δήλωσαν πως τα προσωπικά δεδομένα διατηρούνταν για όσο διάστημα χρειαζόταν (Διάγραμμα 15). Το 47,1% (n=33) ανέφεραν ότι τα προσωπικά δεδομένα διατηρούνταν ακριβή και ενημερωμένα. Το 15,7% (n=11) δήλωσαν πως αυτό δεν συνέβαινε, και το 37,1% (n=26) δήλωσαν πως αυτό συνέβαινε μερικές φορές μόνο (Διάγραμμα 16). Από την άλλη, το 81,4% (n=57) δήλωσαν πως τα προσωπικά δεδομένα διατηρούνταν ασφαλή (Διάγραμμα 17).



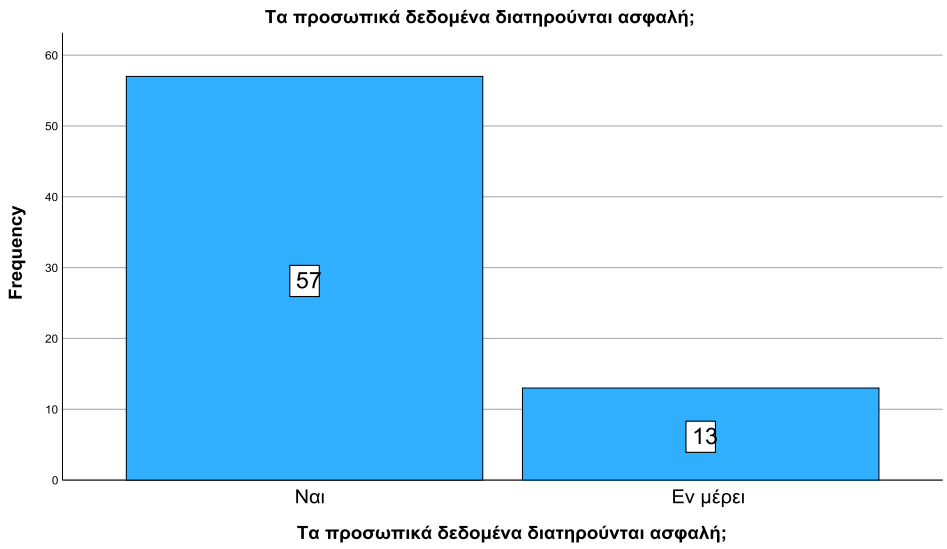
Διάγραμμα 14. Γνώση φυσικών προσώπων για κατοχή και χρήση των προσωπικών δεδομένων τους



Διάγραμμα 15. Χρονική διάρκεια διατήρησης προσωπικών δεδομένων

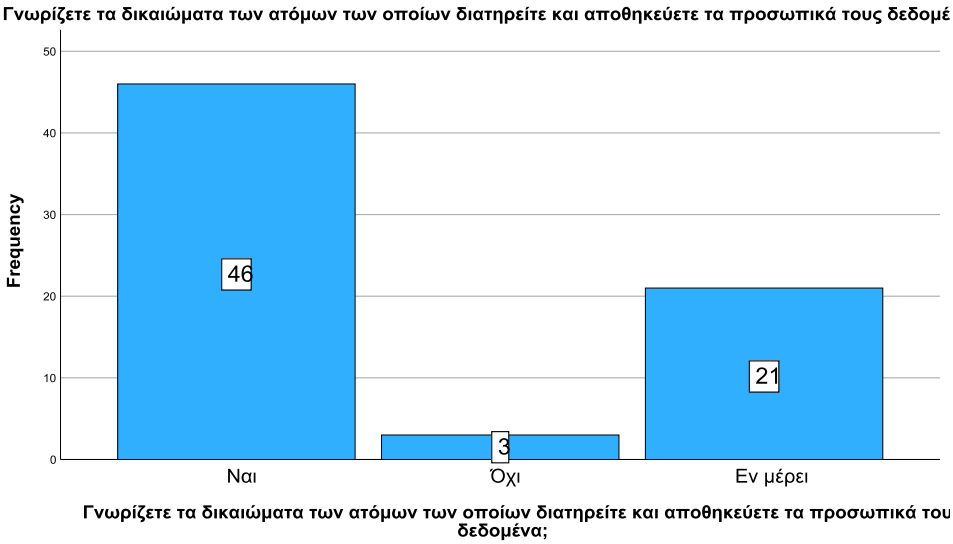


Διάγραμμα 16. Ακρίβεια και ενημέρωση προσωπικών δεδομένων

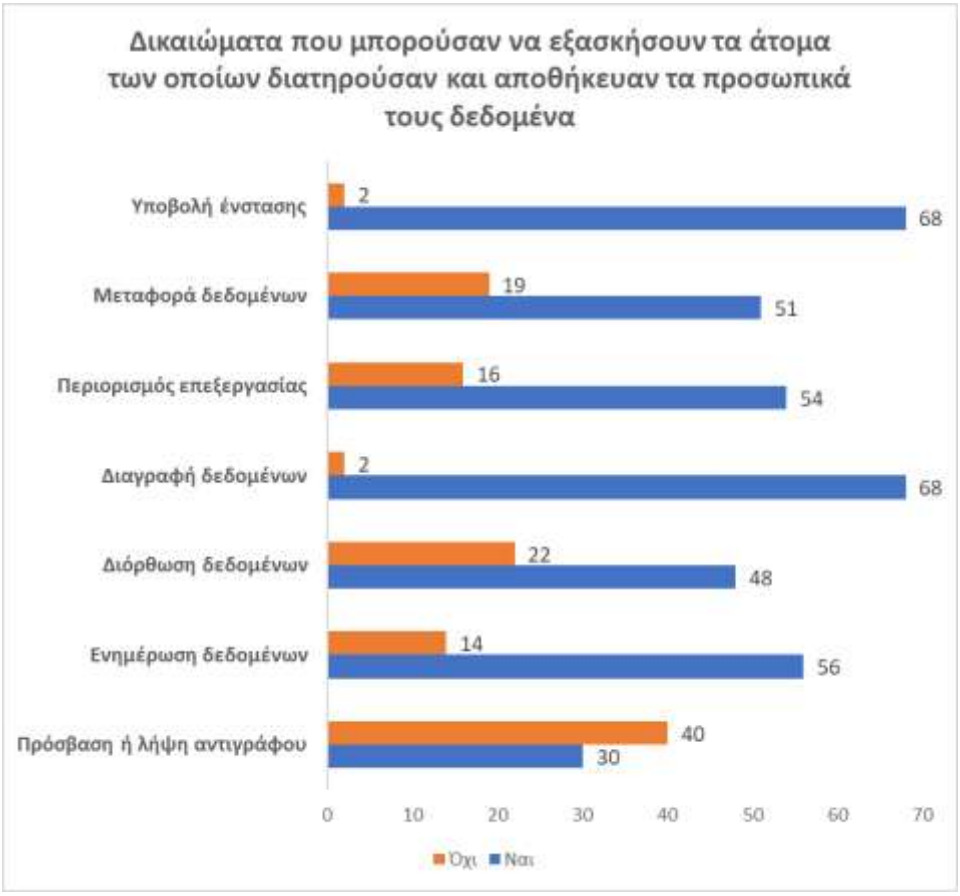


Διάγραμμα 17. Ασφαλής διατήρηση των προσωπικών δεδομένων

Επίσης, το 65,7% (n=46) δήλωσαν ότι γνώριζαν τα δικαιώματα των ατόμων των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα. Το 4,3% (n=3) δήλωσαν πως δεν τα γνώριζαν, ενώ το 30% (n=21) τα γνώριζαν εν μέρει (Διάγραμμα 18). Όσον αφορά τα δικαιώματα που μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα, το 42,9% (n=30) ανέφεραν την πρόσβαση ή λήψη αντιγράφου, το 80% (n=56) ανέφεραν την ενημέρωση δεδομένων, το 68,6% (n=48) ανέφεραν τη διόρθωση δεδομένων, το 97,1% (n=68) ανέφεραν τη διαγραφή δεδομένων, το 77,1% (n=54) ανέφεραν τον περιορισμό επεξεργασίας, το 72,9% (n=51) ανέφεραν τη μεταφορά δεδομένων και το 97,1% (n=68) ανέφεραν την υποβολή ένστασης (Διάγραμμα 19).

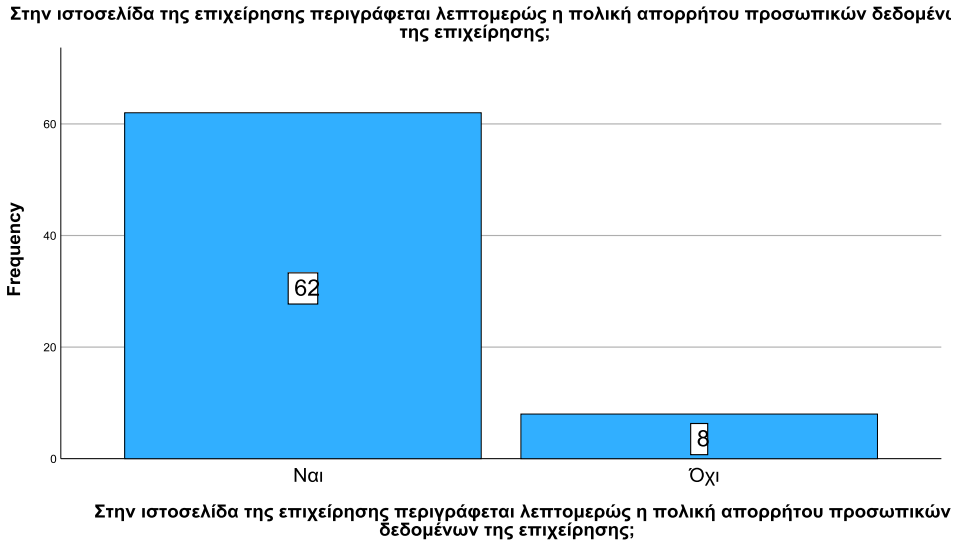


Διάγραμμα 18. Γνώση των δικαιωμάτων των ατόμων των οποίων διατηρούνται και αποθηκεύονται τα προσωπικά τους δεδομένα



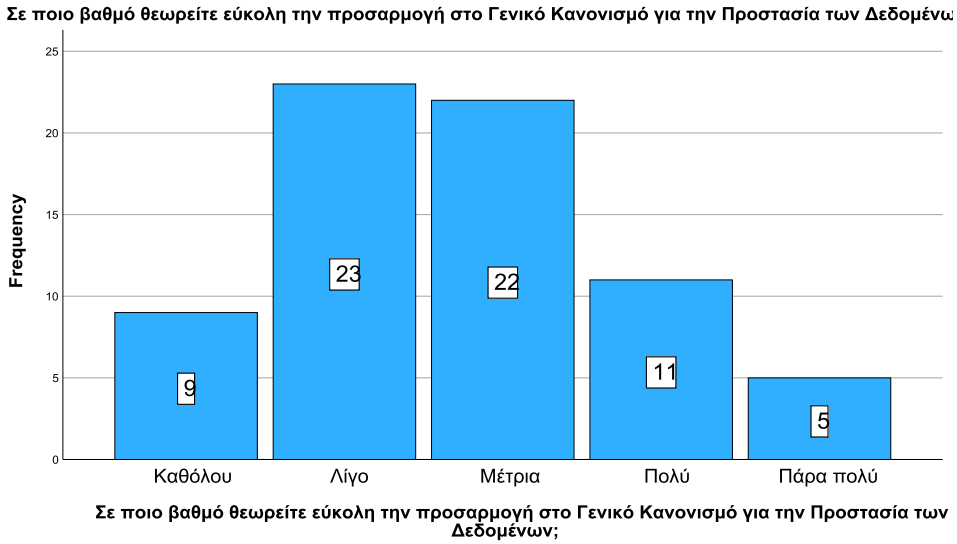
Διάγραμμα 19. Δικαιώματα που μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα

Παράλληλα, το 88,6% (n=62) δήλωσαν πως στην ιστοσελίδα της επιχείρησης περιγραφόταν λεπτομερώς η πολιτική απορρήτου προσωπικών δεδομένων της επιχείρησης (Διάγραμμα 20).

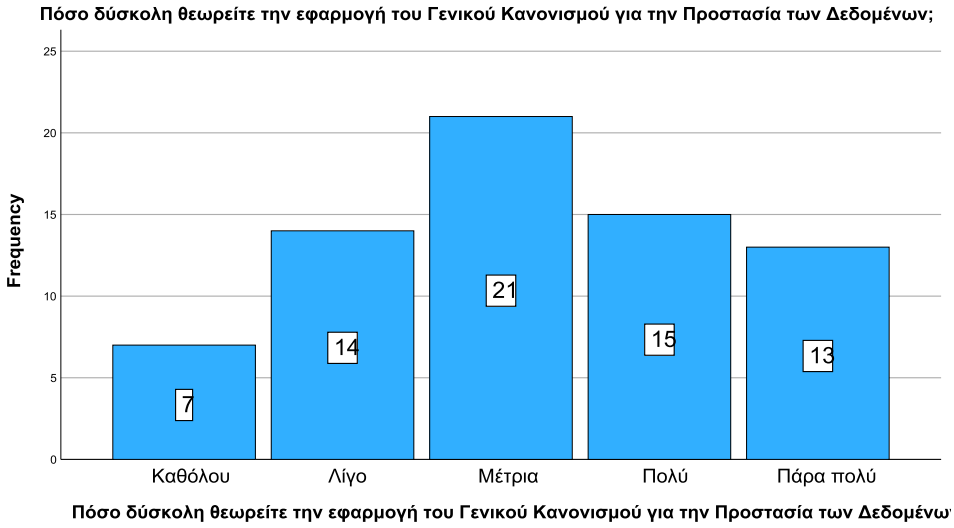


Διάγραμμα 20. Λεπτομερής περιγραφή της πολιτικής απορρήτου προσωπικών δεδομένων στην ιστοσελίδα της επιχείρησης

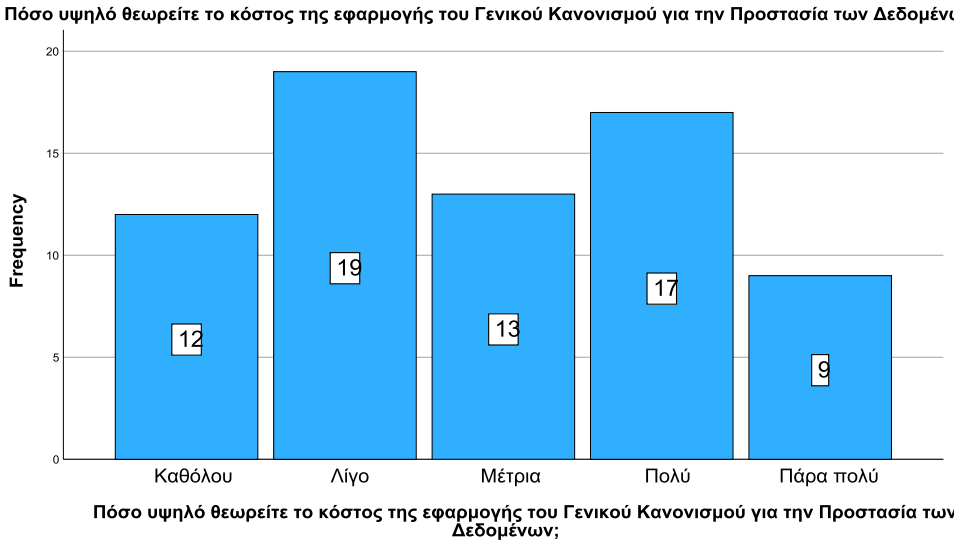
Το 12,9% (n=9) δεν θεωρούσαν καθόλου εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων. Το 32,9% (n=23) τη θεωρούσαν λίγο εύκολη, το 31,4% (n=22) μέτρια εύκολη, το 15,7% (n=11) πολύ εύκολη και το 7,1% (n=5) πάρα πολύ εύκολη (Διάγραμμα 21). Επίσης, το 10% (n=7) δεν θεωρούσαν καθόλου δύσκολη την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Το 20% (n=14) τη θεωρούσαν λίγο δύσκολη, το 30% (n=21) μέτρια δύσκολη, το 21,4% (n=15) πολύ δύσκολη και το 18,6% (n=13) πάρα πολύ δύσκολη (Διάγραμμα 22). Ακόμη, το 17,1% (n=12) δεν θεωρούσαν καθόλου υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Το 27,1% (n=19) το θεωρούσαν λίγο υψηλό, το 18,6% (n=13) μέτρια υψηλό, το 24,3% (n=17) πολύ υψηλό και το 12,9% (n=9) πάρα πολύ υψηλό (Διάγραμμα 23). Παρόμοια, το 14,3% (n=10) δεν πίστευαν καθόλου ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Το 12,9% (n=9) το πίστευαν λίγο, το 38,6% (n=27) μέτρια, το 11,4% (n=8) πολύ και το 22,9% (n=16) πάρα πολύ (Διάγραμμα 24). Παρατηρείται λοιπόν συνολικά ότι οι συμμετέχοντες είχαν μέτριες αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων (Πίνακας 2).



Διάγραμμα 21. Ευκολία προσαρμογής στο Γενικό Κανονισμό για την Προστασία των Δεδομένων



Διάγραμμα 22. Δυσκολία εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων



Διάγραμμα 23. Κόστος εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων

Διάγραμμα 24. Μείωση εσόδων της επιχείρησης εξαιτίας του Γενικού Κανονισμού για την Προστασία των Δεδομένων

Πίνακας 2. Μέσες τιμές και τυπικές αποκλίσεις για τις αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων

	Μέση τιμή	**Τυπική απόκλιση**
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	2,71	1,105
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	3,19	1,243
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	2,89	1,314
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	3,16	1,315

7.2 Επαγωγική στατιστική

Όσον αφορά το φύλο, τόσο με βάση τα Mann-Whitney tests όσο και με βάση τα chi-square tests δεν παρατηρήθηκε καμία στατιστικά σημαντική συσχέτιση ($p > 0.05$ σε όλες τις περιπτώσεις). Παρόμοια, αναφορικά με την ηλικία, το μορφωτικό επίπεδο, τη θέση στην επιχείρηση, το μέγεθος της επιχείρησης, το είδος της επιχείρησης, και τον τομέα δραστηριοποίησης της επιχείρησης, με βάση τα Kruskal-Wallis tests αλλά και τα chi-square tests δεν βρέθηκε καμία στατιστικά σημαντική συσχέτιση ($p > 0.05$ σε όλες τις περιπτώσεις) (βλ. Πίνακες 3-10).

Αναλυτικότερα, διαπιστώθηκε ότι οι άνδρες (mean rank= 36,29) γνώριζαν καλύτερα τον Γενικό Κανονισμό για την Προστασία των Δεδομένων από τις γυναίκες (mean rank= 32,36). Παρόμοια, βρέθηκε ότι οι άνδρες (mean rank= 36,88) θεωρούσαν πιο εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων από τις γυναίκες (mean rank= 29,96). Από την άλλη, οι γυναίκες υποστήριξαν περισσότερο ότι είναι Πόσο δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων και ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Ωστόσο κανένα από αυτά τα αποτελέσματα δεν ήταν στατιστικά σημαντικό ($p > 0,05$) (Πίνακας 3).

Όσον αφορά την ηλικία, διαπιστώθηκε ότι οι εργαζόμενοι έως 30 ετών (mean rank= 38,09) γνώριζαν καλύτερα τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ λιγότερο τον γνώριζαν οι εργαζόμενοι 56-65 ετών (mean rank= 23,09). Παρόμοια, οι εργαζόμενοι 56-65 ετών υποστήριξαν λιγότερο ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων. Ωστόσο, οι εργαζόμενοι έως 30 ετών (mean rank= 47,50) υποστήριξαν περισσότερο ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ενώ η άποψη αυτή υποστηρίχθηκε λιγότερο από τους εργαζομένους 56-65 ετών (mean rank= 31,88). Επιπρόσθετα, οι εργαζόμενοι έως 30 ετών υποστήριξαν λιγότερο ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων και ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Ωστόσο κανένα από αυτά τα αποτελέσματα δεν ήταν στατιστικά σημαντικό ($p > 0,05$) (Πίνακας 4).

Όσον αφορά το μορφωτικό επίπεδο, διαπιστώθηκε ότι οι απόφοιτοι λυκείου γνώριζαν λιγότερο τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, υποστήριξαν λιγότερο ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ υποστήριξαν περισσότερο ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Από την άλλη, οι κάτοχοι διδακτορικού (mean rank= 61,67) υποστήριξαν περισσότερο ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ενώ η άποψη αυτή υποστηρίχθηκε λιγότερο από τους αποφοίτους λυκείου (mean rank= 16,50). Παρόμοια, οι κάτοχοι διδακτορικού υποστήριξαν περισσότερο ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Παρόλα αυτά, κανένα από τα άνωθεν αποτελέσματα δεν ήταν στατιστικά σημαντικό ($p> 0,05$) (Πίνακας 5).

Όσον αφορά τη θέση στην επιχείρηση, διαπιστώθηκε ότι οι μέτοχοι (mean rank= 18,59) γνώριζαν λιγότερο καλά τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ περισσότερο τον γνώριζαν τα στελέχη (mean rank= 44,50). Οι ιδιοκτήτες υποστήριξαν περισσότερο ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ τα στελέχη υποστήριξαν λιγότερο ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων και ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της

επιχείρησης. Ωστόσο κανένα από αυτά τα αποτελέσματα δεν ήταν στατιστικά σημαντικό (p > 0,05) (Πίνακας 6).

Αναφορικά με το είδος της επιχείρησης, διαπιστώθηκε ότι οι εργαζόμενοι σε ιδιωτικές κεφαλαιουχικές εταιρείες γνώριζαν λιγότερο καλά τον Γενικό Κανονισμό για την Προστασία των Δεδομένων και υποστήριξαν περισσότερο ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων. Από την άλλη, οι εργαζόμενοι σε ομόρρυθμες εταιρείες υποστήριξαν περισσότερο ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Οι εργαζόμενοι σε ιδιωτικές κεφαλαιουχικές εταιρείες (mean rank= 53,00) υποστήριξαν περισσότερο ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ενώ οι εργαζόμενοι σε ομόρρυθμες εταιρείες (mean rank= 15,80) υποστήριξαν λιγότερο την άποψη αυτή. Τέλος, οι εργαζόμενοι σε ατομικές εταιρείες υποστήριξαν λιγότερο ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Παρόλα αυτά, κανένα από τα άνωθεν αποτελέσματα δεν ήταν στατιστικά σημαντικό (p> 0,05) (Πίνακας 7).

Όσον αφορά το μέγεθος της επιχείρησης, διαπιστώθηκε ότι οι εργαζόμενοι σε πολύ μικρές επιχειρήσεις γνώριζαν λιγότερο καλά τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, υποστήριξαν λιγότερο ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ υποστήριξαν περισσότερο ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Οι εργαζόμενοι σε μεσαίες επιχειρήσεις (mean rank= 48,27) υποστήριξαν περισσότερο ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ενώ οι εργαζόμενοι σε πολύ μικρές επιχειρήσεις (mean rank= 6,50) υποστήριξαν λιγότερο την άποψη αυτή. Παρόμοια, οι εργαζόμενοι σε μεσαίες επιχειρήσεις υποστήριξαν περισσότερο ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Παρόλα αυτά, κανένα από τα άνωθεν αποτελέσματα δεν ήταν στατιστικά σημαντικό (p> 0,05) (Πίνακας 8).

Όσον αφορά τον τομέα δραστηριοποίησης της επιχείρησης, διαπιστώθηκε ότι οι εργαζόμενοι σε επιχειρήσεις με μεταποίηση (mean rank= 53,80) γνώριζαν καλύτερα τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ λιγότερο καλά τον γνώριζαν οι εργαζόμενοι σε επιχειρήσεις που δραστηριοποιούνται σε κατασκευές (mean rank= 19,25). Οι εργαζόμενοι σε επιχειρήσεις που δραστηριοποιούνται σε κατασκευές υποστήριξαν λιγότερο

ότι είναι εύκολη η προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ενώ η άποψη ότι είναι δύσκολη η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων υποστηρίχθηκε λιγότερο από τους εργαζομένους σε τουριστικές επιχειρήσεις. Οι εργαζόμενοι σε επιχειρήσεις που δραστηριοποιούνται στο εμπόριο υποστήριξαν περισσότερο ότι είναι υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ενώ οι εργαζόμενοι σε επιχειρήσεις που δραστηριοποιούνται στην μεταποίηση υποστήριξαν περισσότερο ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης. Παρόλα αυτά, κανένα από τα άνωθεν αποτελέσματα δεν ήταν στατιστικά σημαντικό ($p > 0,05$) (Πίνακας 9).

Από την άλλη, με βάση τα chi-square tests διαπιστώθηκε ότι τα δημογραφικά χαρακτηριστικά και τα στοιχεία της επιχείρησης (φύλο, ηλικία, μορφωτικό επίπεδο, θέση στην επιχείρηση, είδος επιχείρησης, μέγεθος επιχείρησης, τομέας δραστηριοποίησης επιχείρησης) δεν σχετίζονταν στατιστικά σημαντικά με το εάν έχει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων, με το εάν διατηρούνται τα προσωπικά δεδομένα πελατών, συνεργατών, προμηθευτών και υπαλλήλων, εάν διαμοιράζονται τα προσωπικά δεδομένα που διατηρούνται με άλλους οργανισμούς και επιχειρήσεις, εάν γίνεται χρήση των προσωπικών δεδομένων που διατηρούνται για προωθητικές ενέργειες πωλήσεων, εάν όταν αποστέλλονται email ή SMS στα άτομα των οποίων διατηρούνται τα προσωπικά τους δεδομένα, δίνεται η δυνατότητα διακοπής της επικοινωνίας (διαγραφή) με κατανοητό και απλό τρόπο. Επίσης, τα δημογραφικά χαρακτηριστικά και τα στοιχεία της επιχείρησης δεν σχετίζονταν στατιστικά σημαντικά με το εάν τα φυσικά πρόσωπα γνωρίζουν ότι έχουν τα προσωπικά τους δεδομένα και τον λόγο και τον τρόπο χρήσης τους, με το εάν τα προσωπικά δεδομένα διατηρούνται για όσο διάστημα χρειάζεται, με το εάν τα προσωπικά δεδομένα διατηρούνται ακριβή και ενημερωμένα, με το εάν τα προσωπικά δεδομένα διατηρούνται ασφαλή, με το εάν οι εργαζόμενοι γνώριζαν τα δικαιώματα των ατόμων των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα, ούτε με το ποια δικαιώματα μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα, ούτε με το εάν στην ιστοσελίδα της επιχείρησης περιγράφεται λεπτομερώς η πολική απορρήτου προσωπικών δεδομένων της επιχείρησης. Σε όλες τις περιπτώσεις διαπιστώθηκε ότι $p > 0,05$ (Πίνακας 10).

Πίνακας 3. Mann-Whitney tests για διερεύνηση διαφοροποιήσεων ανάλογα το φύλο

	Φύλο	Mean Rank	p
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Άνδρας	36,29	,497
	Γυναίκα	32,36	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Άνδρας	36,88	,237
	Γυναίκα	29,96	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Άνδρας	33,20	,062
	Γυναίκα	44,71	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Άνδρας	33,14	,087
	Γυναίκα	44,93	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Άνδρας	33,09	,099
	Γυναίκα	45,14	

Πίνακας 4. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα την ηλικία

	Ηλικία	Mean Rank	p
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Έως 30 ετών	38,09	,679
	31-45 ετών	32,33	
	46-55 ετών	37,31	
	56-65 ετών	23,09	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Έως 30 ετών	36,88	,253
	31-45 ετών	41,04	
	46-55 ετών	30,96	
	56-65 ετών	26,00	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Έως 30 ετών	47,50	,469
	31-45 ετών	33,24	
	46-55 ετών	38,37	
	56-65 ετών	31,88	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Έως 30 ετών	17,00	,109
	31-45 ετών	28,28	
	46-55 ετών	46,30	
	56-65 ετών	27,26	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού	Έως 30 ετών	34,67	,355
	31-45 ετών	44,35	

για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	46-55 ετών	38,04	
	56-65 ετών	50,24	

Πίνακας 5. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το μορφωτικό επίπεδο

	Μορφωτικό επίπεδο	**Mean Rank**	**p**
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Απόφοιτος λυκείου	14,00	,288
	Απόφοιτος ΑΕΙ/ΤΕΙ	50,65	
	Κάτοχος μεταπτυχιακού	31,46	
	Κάτοχος διδακτορικού	35,00	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Απόφοιτος λυκείου	5,00	,448
	Απόφοιτος ΑΕΙ/ΤΕΙ	36,38	
	Κάτοχος μεταπτυχιακού	43,50	
	Κάτοχος διδακτορικού	39,50	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Απόφοιτος λυκείου	64,00	,091
	Απόφοιτος ΑΕΙ/ΤΕΙ	27,83	
	Κάτοχος μεταπτυχιακού	30,72	
	Κάτοχος διδακτορικού	36,33	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Απόφοιτος λυκείου	16,50	,062
	Απόφοιτος ΑΕΙ/ΤΕΙ	18,43	
	Κάτοχος μεταπτυχιακού	40,57	
	Κάτοχος διδακτορικού	61,67	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Απόφοιτος λυκείου	25,50	,321
	Απόφοιτος ΑΕΙ/ΤΕΙ	43,53	
	Κάτοχος μεταπτυχιακού	34,88	
	Κάτοχος διδακτορικού	47,58	

Πίνακας 6. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα τη θέση στην επιχείρηση

	Θέση στην επιχείρηση	Mean Rank	p
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Ιδιοκτήτης	25,13	,109
	Διευθυντής	41,76	
	Στέλεχος	44,50	
	Μέτοχος	18,41	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Ιδιοκτήτης	51,63	,124
	Διευθυντής	22,71	
	Στέλεχος	42,62	
	Μέτοχος	18,59	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Ιδιοκτήτης	51,63	,238
	Διευθυντής	47,38	
	Στέλεχος	16,48	
	Μέτοχος	32,56	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Ιδιοκτήτης	44,38	,331
	Διευθυντής	43,90	
	Στέλεχος	24,00	
	Μέτοχος	48,25	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Ιδιοκτήτης	44,38	,246
	Διευθυντής	40,52	
	Στέλεχος	18,52	
	Μέτοχος	27,38	

Πίνακας 7. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το είδος της επιχείρησης

	Είδος επιχείρησης	Mean Rank	p
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Ατομική εταιρεία	22,65	,298
	Ομόρρυθμη εταιρεία	22,90	
	Ετερόρρυθμη εταιρεία	58,50	
	Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία	53,28	
	Περιορισμένης ευθύνης εταιρεία	40,22	
	Ιδιωτική κεφαλαιουχική εταιρεία	12,31	
	Ανώνυμη εταιρεία	39,56	
Σε ποιο βαθμό	Ατομική εταιρεία	22,05	,417

θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Ομόρρυθμη εταιρεία	26,90	
	Ετερόρρυθμη εταιρεία	28,50	
	Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία	21,00	
	Περιορισμένης ευθύνης εταιρεία	38,50	
	Ιδιωτική κεφαλαιουχική εταιρεία	53,81	
	Ανώνυμη εταιρεία	41,48	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Ατομική εταιρεία	51,20	,225
	Ομόρρυθμη εταιρεία	57,60	
	Ετερόρρυθμη εταιρεία	48,67	
	Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία	46,00	
	Περιορισμένης ευθύνης εταιρεία	35,56	
	Ιδιωτική κεφαλαιουχική εταιρεία	5,31	
	Ανώνυμη εταιρεία	29,33	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Ατομική εταιρεία	20,20	,096
	Ομόρρυθμη εταιρεία	15,80	
	Ετερόρρυθμη εταιρεία	16,83	
	Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία	31,78	
	Περιορισμένης ευθύνης εταιρεία	51,33	
	Ιδιωτική κεφαλαιουχική εταιρεία	53,00	
	Ανώνυμη εταιρεία	37,75	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Ατομική εταιρεία	16,65	,144
	Ομόρρυθμη εταιρεία	18,80	
	Ετερόρρυθμη εταιρεία	46,67	
	Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία	62,50	
	Περιορισμένης ευθύνης εταιρεία	53,17	
	Ιδιωτική κεφαλαιουχική εταιρεία	21,75	
	Ανώνυμη εταιρεία	33,44	

Πίνακας 8. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα το μέγεθος της επιχείρησης

	Μέγεθος επιχείρησης	**Mean Rank**	**p**
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Πολύ μικρή	14,00	,111
	Μικρή	31,12	
	Μεσαία	33,77	
	Μεγάλη	41,90	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο	Πολύ μικρή	5,00	,167
	Μικρή	15,35	

Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Μεσαία	39,97	
	Μεγάλη	43,19	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Πολύ μικρή	64,00	,141
	Μικρή	58,31	
	Μεσαία	29,18	
	Μεγάλη	28,94	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Πολύ μικρή	6,50	,209
	Μικρή	13,65	
	Μεσαία	48,27	
	Μεγάλη	33,25	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Πολύ μικρή	5,50	,123
	Μικρή	31,81	
	Μεσαία	38,06	
	Μεγάλη	36,69	

Πίνακας 9. Kruskal-Wallis tests για διερεύνηση διαφοροποιήσεων ανάλογα τον τομέα δραστηριοποίησης της επιχείρησης

	Τομέας δραστηριοποίησης επιχείρησης	**Mean Rank**	**p**
Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Κατασκευές	19,25	,064
	Μεσιτικά	35,09	
	Μεταποίηση	53,80	
	Εμπόριο	37,36	
	Εφοδιαστική αλυσίδα και μεταφορές	24,46	
	Τουρισμός	21,42	
	Χρηματοοικονομικές υπηρεσίες	52,63	
	Πληροφορική και επικοινωνίες	50,67	
Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;	Κατασκευές	9,00	,098
	Μεσιτικά	20,14	
	Μεταποίηση	25,50	
	Εμπόριο	36,82	
	Εφοδιαστική αλυσίδα και μεταφορές	46,85	
	Τουρισμός	64,00	
	Χρηματοοικονομικές	50,13	

	υπηρεσίες		
	Πληροφορική και επικοινωνίες	38,79	
Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Κατασκευές	58,25	,124
	Μεσιτικά	56,36	
	Μεταποίηση	49,20	
	Εμπόριο	35,27	
	Εφοδιαστική αλυσίδα και μεταφορές	20,77	
	Τουρισμός	17,42	
	Χρηματοοικονομικές υπηρεσίες	23,25	
	Πληροφορική και επικοινωνίες	24,79	
Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;	Κατασκευές	18,13	,222
	Μεσιτικά	22,00	
	Μεταποίηση	25,10	
	Εμπόριο	51,64	
	Εφοδιαστική αλυσίδα και μεταφορές	50,04	
	Τουρισμός	42,83	
	Χρηματοοικονομικές υπηρεσίες	22,25	
	Πληροφορική και επικοινωνίες	34,00	
Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;	Κατασκευές	12,38	,073
	Μεσιτικά	41,59	
	Μεταποίηση	56,60	
	Εμπόριο	44,32	
	Εφοδιαστική αλυσίδα και μεταφορές	33,73	
	Τουρισμός	30,00	
	Χρηματοοικονομικές υπηρεσίες	35,88	
	Πληροφορική και επικοινωνίες	33,00	

Πίνακας 10. Chi-square tests για τη διερεύνηση διαφοροποιήσεων ανάλογα τα δημογραφικά χαρακτηριστικά

	Φύλο	**Ηλικία**	**Μορφωτικό επίπεδο**	**Θέση στην επιχείρηση**	**Είδος επιχείρησης**	**Μέγεθος επιχείρησης**	**Τομέας δραστηριο-ποίησης επιχείρησης**
Έχει γίνει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων;	,208	,421	,587	,118	,561	,094	,065
Διατηρούνται τα προσωπικά δεδομένα πελατών, συνεργατών, προμηθευτών και υπαλλήλων (δηλ. ονοματεπώνυμο, διεύθυνση, κινητό τηλέφωνο, email κλπ);	,201	,060	,116	,341	,700	,132	,076
Διαμοιράζονται τα προσωπικά δεδομένα που διατηρούνται με άλλους οργανισμούς και επιχειρήσεις;	,136	,078	,076	,336	,297	,218	,079
Γίνεται χρήση των προσωπικών δεδομένων που διατηρούνται για προωθητικές ενέργειες πωλήσεων;	,204	,120	,323	,703	,314	,292	,244
Όταν αποστέλλονται email ή	,600	,177	,333	,890	,325	,265	,222

SMS στα άτομα των οποίων διατηρείτε τα προσωπικά τους δεδομένα, δίνεται η δυνατότητα διακοπής της επικοινωνίας (διαγραφή) με κατανοητό και απλό τρόπο;							
Τα φυσικά πρόσωπα γνωρίζουν ότι έχετε τα προσωπικά τους δεδομένα και τον λόγο και τον τρόπο χρήσης τους;	,204	,120	,323	,454	,835	,670	,121
Τα προσωπικά δεδομένα διατηρούνται για όσο διάστημα χρειάζεται;	,428	,065	,112	,593	,147	,826	,087
Τα προσωπικά δεδομένα διατηρούνται ακριβή και ενημερωμένα;	,565	,090	,133	,898	,075	,138	,413
Τα προσωπικά δεδομένα διατηρούνται ασφαλή;	,204	,708	,790	,398	,094	,060	,291
Γνωρίζετε τα δικαιώματα των ατόμων των οποίων διατηρείτε και αποθηκεύετε τα προσωπικά τους δεδομένα;	,307	,918	,551	,428	,078	,094	,068
Πρόσβαση ή λήψη αντιγράφου	,336	,088	,197	,818	,327	,132	,115
Ενημέρωση δεδομένων	,565	,114	,133	,738	,657	,218	,322
Διόρθωση δεδομένων	,476	,110	,467	,749	,835	,292	,107
Διαγραφή δεδομένων	,178	,948	,405	,385	,140	,265	,291
Περιορισμός επεξεργασίας	,221	,974	,464	,264	,075	,670	,068

Μεταφορά δεδομένων	,428	,065	,112	,891	,094	,095	,115
Υποβολή ένστασης	,476	,110	,290	,241	,144	,414	,300
Στην ιστοσελίδα της επιχείρησης περιγράφεται λεπτομερώς η πολική απορρήτου προσωπικών δεδομένων της επιχείρησης;	,308	,092	,308	,185	,657	,859	,456

Κεφάλαιο 8ο: Συζήτηση

Η έρευνα αυτή διερεύνησε το βαθμό συμμόρφωσης των επιχειρήσεων με το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων.

Διαπιστώθηκε ότι οι επιχειρηματίες γνώριζαν ικανοποιητικά το Γενικό Κανονισμό για την Προστασία των Δεδομένων. Ακόμη, η πλειοψηφία των επιχειρηματιών γνώριζαν τα δικαιώματα των ατόμων των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα.

Μια σημαντική πρόκληση που σχετίζεται με την εφαρμογή του GDPR είναι η έλλειψη ενημέρωσης και κατανόησης από τις εταιρείες για τις επικείμενες αλλαγές και απαιτήσεις που επιβάλλει ο GDPR μέσω των νέων κανόνων του. Αυτές οι απαιτήσεις έχουν διάφορες πρακτικές επιπτώσεις για τις οργανωτικές διαδικασίες και πρακτικές, τον σχεδιασμό τεχνολογικών συστημάτων, καθώς και την εκπαίδευση του προσωπικού και την ανάθεση νέων ευθυνών στους οργανισμούς (Tikkinen-Piri, Rohunen & Markkula, 2018). Τέτοιες απαιτήσεις αναδεικνύουν την ανάγκη αναθεώρησης των τρεχουσών πρακτικών απορρήτου δεδομένων και τεχνολογικών μέτρων προστασίας δεδομένων, καθώς και πιθανού σχεδιασμού νέων για τη διασφάλιση της συμμόρφωσης με τον GDPR. Ορισμένες εταιρείες κατανοούν την ανάγκη για αλλαγές, αλλά η έρευνα δείχνει ότι οι πληροφορίες σχετικά με τον GDPR και τις διατάξεις του δεν διαδίδονται απαραίτητα σε αυτές έγκαιρα. Σύμφωνα με τις έρευνες των London Economics (2013), Mikkonen (2014) και TRUSTe (2015), λιγότερες από τις μισές εταιρείες γνώριζαν τις αλλαγές του GDPR. Η εκμάθηση και η κατανόηση των νομοθετικών απαιτήσεων καθαυτών είναι συχνά επαχθής και χρονοβόρα, με αποτέλεσμα να δημιουργούνται δυσκολίες στην εφαρμογή των διατάξεων της νομοθεσίας.

Η εφαρμογή του GDPR απαιτεί αλλαγές που έχουν ποικίλες επιπτώσεις για τις εταιρείες και τη χρήση των πόρων τους. Για παράδειγμα, η συμμόρφωση με τον GDPR επηρεάζει έντονα τις μικρές και μεσαίες επιχειρήσεις με ένταση πληροφοριών που οδηγούν στην αύξηση των εσόδων τους από τη διαδικτυακή διαφήμιση (Thüsing & Traut, 2013). Αυτές οι εταιρείες επίσης δεν μπορούν απαραίτητα να αντέξουν οικονομικά τη νομική βοήθεια για να συμμορφωθούν με τους νέους κανόνες του GDPR. Καθώς η μη συμμόρφωση με τον GDPR εγκυμονεί οικονομικούς, νομικούς και κινδύνους φήμης για τις εταιρείες, μπορεί να

θελήσουν να αντιμετωπίσουν τις απαιτήσεις του GDPR μέσω των πολιτικών διαχείρισης κινδύνου και των αναλύσεων κινδύνου. Με αυτόν τον τρόπο, τα ζητήματα απορρήτου δεδομένων μπορούν να αντιμετωπιστούν μέσω των καθιερωμένων διαδικασιών διαχείρισης κινδύνων από τις εταιρείες (Tikkinen-Piri, Rohunen & Markkula, 2018).

Παρόλα αυτά, η τρέχουσα μελέτη βρήκε μέτριο βαθμός συμμόρφωσης στο Γενικό Κανονισμό για την Προστασία των Δεδομένων. Η πλειοψηφία των επιχειρηματιών υπογράμμισε πως διατηρούνταν τα προσωπικά δεδομένων πελατών, συνεργατών, προμηθευτών και υπαλλήλων, αλλά δεν διαμοιράζονταν τα προσωπικά δεδομένα με άλλους οργανισμούς και επιχειρήσεις. Οι περισσότερες επιχειρήσεις χρησιμοποιούσαν τα προσωπικά δεδομένα για προωθητικές ενέργειες πωλήσεων και όταν αποστέλλονταν email ή SMS στα άτομα των οποίων διατηρούνταν τα προσωπικά τους δεδομένα, δινόταν η δυνατότητα διαγραφής με κατανοητό και απλό τρόπο. Υποστηρίχθηκε επίσης ότι στις περισσότερες επιχειρήσεις τα φυσικά πρόσωπα γνώριζαν για την κατοχή των προσωπικών δεδομένων και τον τρόπο χρήσης τους, ότι τα προσωπικά δεδομένα διατηρούνταν για όσο διάστημα χρειάζεται, και ότι τα προσωπικά δεδομένα διατηρούνταν σε μέτριο βαθμό ακριβή και ενημερωμένα, αλλά διατηρούνταν σε μεγάλο βαθμό ασφαλή. Όσον αφορά τα δικαιώματα που μπορούσαν να εξασκήσουν τα άτομα των οποίων διατηρούσαν και αποθήκευαν τα προσωπικά τους δεδομένα, σχεδόν σε όλες τις επιχειρήσεις υπήρχε η υποβολή ένστασης και η διαγραφή δεδομένων, ενώ σε αρκετές υπήρχε η μεταφορά δεδομένων, ο περιορισμός επεξεργασίας, και η ενημέρωση δεδομένων, ενώ σε ακόμη λιγότερες επιχειρήσεις υπήρχε το δικαίωμα διόρθωσης δεδομένων και το δικαίωμα πρόσβασης ή λήψης αντιγράφου. Παράλληλα, οι περισσότεροι επιχειρηματίες δήλωσαν πως στην ιστοσελίδα της επιχείρησης περιγραφόταν λεπτομερώς η πολιτική απορρήτου προσωπικών δεδομένων της επιχείρησης. Επιπρόσθετα, είναι σημαντικό να αναφερθεί ότι πολύ λίγοι επιχειρηματίες δήλωσαν πώς είχε γίνει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων.

Με βάση την πρόσφατη έρευνα του Piwik (2023) με δείγμα 300 επιχειρηματίες από 30 χώρες της Ευρωπαϊκής Ένωσης, η πλειοψηφία των επιχειρήσεων έβρισκαν ισορροπία μεταξύ αποτελεσματικού μάρκετινγκ και συμμόρφωσης με την προστασία προσωπικών δεδομένων. Οι επιχειρήσεις λάμβαναν επίσης πιο σοβαρά υπόψη τις αξιολογήσεις απορρήτου της τεχνολογίας τους. Η συντριπτική πλειοψηφία των συμμετεχόντων στη μελέτη πίστευε ότι οι επιχειρήσεις πρέπει να σέβονται το διαδικτυακό απόρρητο των ατόμων, και οι περισσότεροι

ερωτηθέντες τόνισαν επίσης τον σεβασμό του διαδικτυακού απορρήτου των ατόμων ως ηθική και νομική υποχρέωση.

Επιπλέον, η τρέχουσα μελέτη έδειξε ότι οι επιχειρηματίες είχαν μέτριες αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων. Συγκεκριμένα, οι επιχειρηματίες υποστήριξαν σε μέτριο βαθμό ότι είναι εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, ότι θεωρούν δύσκολη την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, ότι θεωρούν υψηλό το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων και ότι πιστεύουν ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης.

Η Guseva και οι συνεργάτες της (2022) ανέφεραν ότι ο βαθμός προστασίας των προσωπικών δεδομένων των πελατών επηρεάζει άμεσα τις οικονομικές επιδόσεις των εταιρειών. Επίσης, σύμφωνα με τους Martin, Borah και Palmatier (2017), η διαφάνεια και ο έλεγχος στις πρακτικές διαχείρισης δεδομένων των επιχειρήσεων μπορεί να καταστείλει τις αρνητικές επιπτώσεις της ευπάθειας των δεδομένων πελατών. Ακόμη, στην έρευνα του Piwik (2023), μεγάλο μέρος των επιχειρηματιών πίστευε ότι το διαδικτυακό απόρρητο επηρεάζει θετικά τις επιχειρήσεις και μπορεί να εκληφθεί ως επιχειρηματικό πλεονέκτημα, ενώ οι περισσότεροι επιχειρηματίες αναγνώρισαν ότι η συμμόρφωση με τα πρότυπα απορρήτου στο διαδίκτυο μπορεί να είναι πρόκληση, και υποστήριξαν ότι οι απαιτήσεις του GDPR ήταν εύκολο να κατανοηθούν, και ότι οι απαιτήσεις του GDPR είναι εύκολο να εφαρμοστούν. Στην ίδια έρευνα, διαπιστώθηκε ότι οι περισσότεροι επιχειρηματίες δήλωσαν πως η συμμόρφωση με τον GDPR δεν έχει επηρεάσει αρνητικά την επιχείρησή τους. Μεταξύ των αρνητικών συνεπειών του νόμου, οι επιχειρηματίες ανέφεραν υψηλότερο κόστος αποθήκευσης και διαχείρισης δεδομένων, τεράστιο φόρτο εργασίας και περιορισμένες ευκαιρίες μάρκετινγκ, συμπεριλαμβανομένων δραστηριοτήτων που σχετίζονται με την εξατομίκευση και τη χρήση τεχνητής νοημοσύνης.

Από τη άλλη, ο Demirer και οι συνεργάτες του (2023) έδειξαν ότι η συμμόρφωση στον GDPR ισοδυναμούσε με φόρο 20% στο κόστος αποθήκευσης δεδομένων, ενώ ο Koutroumpis και οι συνεργάτες του (2022) διαπίστωσαν ότι η ζήτηση για εργασία που σχετίζεται με τον κυβερνοχώρο αυξήθηκε κατά 52% σε περισσότερο ελεγμένους τομείς. Η έρευνα από τον Maex (2022) διαπίστωσε ότι ο GDPR βελτίωσε τους δείκτες πληροφόρησης της εσωτερικής ποιότητας πληροφοριών των επιχειρήσεων, οι οποίοι βελτίωσαν έμμεσα τη

λειτουργική αποτελεσματικότητα των επιχειρήσεων (δηλαδή την αποτελεσματικότητα της ανάπτυξης εισροών για τη δημιουργία πωλήσεων). Ωστόσο, ο Maex (2022) διαπίστωσε ότι το ρυθμιστικό βάρος του GDPR ξεπέρασε αυτό το όφελος, έτσι ώστε η λειτουργική αποτελεσματικότητα των εταιρειών έπεσε στο καθαρό. Επίσης, οι Koski και Valmari (2020) έδειξαν ότι το κόστος του GDPR κατά το πρώτο έτος εφαρμογής του ήταν σημαντικό, τουλάχιστον για ορισμένες ευρωπαϊκές εταιρείες. Τα περιθώρια κέρδους των επιχειρήσεων αυξήθηκαν, κατά μέσο όρο, κατά περίπου 1,7 έως 3,4 ποσοστιαίες μονάδες λιγότερο από τα περιθώρια κέρδους των ομολόγων τους στις ΗΠΑ. Οι ευρωπαϊκές μικρομεσαίες επιχειρήσεις ήταν η πιο μειονεκτική ομάδα όσον αφορά τις εξελίξεις κερδών τους μετά τον GDPR, ενώ τα βραχυπρόθεσμα περιθώρια κέρδους των μεγάλων ευρωπαϊκών εταιρειών μειώθηκαν σχετικά λιγότερο (Koski & Valmari, 2020).

Επιπρόσθετα, η παρούσα έρευνα διαπιστώθηκε ότι δεν υπήρχαν διαφοροποιήσεις στο βαθμό συμμόρφωσης και τις αντιλήψεις για το Γενικό Κανόνα για την Προστασία των Προσωπικών Δεδομένων ανάλογα το φύλο, την ηλικία, το μορφωτικό επίπεδο και τη θέση στην επιχείρηση των επιχειρηματιών, ούτε ανάλογα το είδος, το μέγεθος και τον τομέα δραστηριοποίησης της επιχείρησης.

Σύμφωνα με τον Brodin (2019) οι μικρές και οι μεσαίες επιχειρήσεις έχουν μικρότερο βαθμό συμμόρφωσης στο Γενικό Κανόνα για την Προστασία των Δεδομένων. Για τις μικρές και μεσαίες επιχειρήσεις, τα μεγάλα δεδομένα παρουσιάζουν σημαντικές ευκαιρίες και προκλήσεις. Οι επιχειρήσεις αυτές γνωρίζουν καλά τους πελάτες τους, αλλά έχουν περιορισμένη ικανότητα συλλογής και ανάλυσης δεδομένων. Επιπλέον, το όφελος από τη χρήση της τεχνολογίας μεγάλων δεδομένων γίνεται πιο εμφανές καθώς αυξάνεται ο όγκος και η ποικιλία των δεδομένων. Για τις μικρές επιχειρήσεις ή οργανισμούς, η ανεξάρτητα επίτευξη των τεσσάρων έναντι των μεγάλων δεδομένων, δηλαδή η ταχύτητα, ο όγκος, η ποικιλία και η ακρίβεια, είναι πρόκληση. Η σημαντική τεχνολογική ικανότητα, ο αριθμός των χρηστών και η ποικιλία των υπηρεσιών τεχνολογικών κολοσσών όπως η Google και το Facebook εξοπλίζουν καλύτερα αυτές τις επιχειρήσεις για να επιτύχουν αυτούς τους στόχους. Παρά τα εμπόδια αυτά, οι μικρές και οι μεσαίες επιχειρήσεις μπορούν να βρουν μεθόδους για να συμβαδίζουν με τους μεγαλύτερους ομολόγους τους στον αγώνα μεγάλων δεδομένων. Για να ξεπεραστούν οι περιορισμοί πόρων και χωρητικότητας, η ανάθεση δραστηριοτήτων στην αλυσίδα αξίας των μεγάλων δεδομένων όπως η ανάλυση και η οπτικοποίηση σε οργανισμούς με σχετική τεχνογνωσία αποτελεί μια βιώσιμη στρατηγική. Για να αυξηθεί ο όγκος και η

ποικιλία δεδομένων, η κοινή χρήση δεδομένων ή η συλλογική ανάλυση δεδομένων μεταξύ των υπευθύνων επεξεργασίας δεδομένων μπορεί να ωφελήσει την ομάδα ως σύνολο. Εν ολίγοις, οι μικροί οργανισμοί μπορούν να ενισχύσουν την ανταγωνιστικότητά τους μέσω της διοργανωτικής ανάλυσης δεδομένων (Del Vecchio et al., 2018; Wang & Wang, 2020; Li, Chen & Huang, 2021). Τέλος, ο Marikyan και οι συνεργάτες του (2022) έδειξαν ότι η αντιληπτή σοβαρότητα της απειλής, η αυτο-αποτελεσματικότητα και η αποτελεσματικότητα απόκρισης καθορίζουν μια θετική στάση απέναντι στη συμμόρφωση με τον GDPR, η οποία οδηγεί σε συναισθηματική ενδυνάμωση.

Τέλος, η παρούσα μελέτη διακατέχεται από κάποιους περιορισμούς. Το δείγμα της έρευνας είναι μικρό, επομένως δεν καθίσταται δυνατή η γενίκευση των αποτελεσμάτων. Επίσης, καθώς το δείγμα προερχόταν από επιχειρηματίες και χρησιμοποιήθηκε δειγματοληψία ευκολίας, πιθανόν να υπάρχει κίνδυνος μεροληψίας, ο οποίος ενδεχομένως να ήταν μικρότερος εάν το δείγμα αποτελούνταν από εργαζομένους των επιχειρήσεων αυτών. Επιπλέον, δεν μελετήθηκε εάν ο βαθμός συμμόρφωσης στο Γενικό Κανόνα για την Προστασία των Δεδομένων σχετίζονταν με τις αντιλήψεις των επιχειρηματιών για το Γενικό Κανόνα για την Προστασία των Δεδομένων. Ακόμη, μια ποιοτικής φύσεως έρευνα θα φώτιζε καλύτερα τις αντιλήψεις των επιχειρηματιών για τα πλεονεκτήματα, τα μειονεκτήματα και τις προκλήσεις κατά την εφαρμογή του Γενικού Κανόνα για την Προστασία των Δεδομένων.

Συμπεράσματα

Τα τελευταία χρόνια, τα δεδομένα έχουν γίνει σημαντικό θέμα συζήτησης και οι επιχειρήσεις πρέπει πλέον να αφιερώνουν σημαντικούς πόρους για τη συμμόρφωση με τους κανονισμούς και την προστασία των δεδομένων που συλλέγουν. Η ανάγκη για συμμόρφωση με τους διεθνείς κανονισμούς προστασίας δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης, επιβάλλει νέες προκλήσεις και απαιτήσεις για τους οργανισμούς, απαιτώντας από αυτούς να ενσωματώσουν αυστηρά πρωτόκολλα και διαδικασίες για την προστασία των δεδομένων. Η διαχείριση και η προστασία των προσωπικών δεδομένων δεν αποτελεί μόνο νομική υποχρέωση, αλλά επιβάλλεται και ως ηθική επιταγή, αναδεικνύοντας την ανάγκη για συνεχή ενημέρωση, προσαρμογή και βελτίωση των εσωτερικών μηχανισμών ασφάλειας και προστασίας δεδομένων. Οι συνεχείς τεχνολογικές εξελίξεις και η αλλαγή του ψηφιακού τοπίου προσθέτουν επιπλέον πολυπλοκότητα στην εφαρμογή και την τήρηση των κανονισμών. Η ανάλυση των προκλήσεων, των βέλτιστων πρακτικών και των στρατηγικών για την αποτελεσματική συμμόρφωση με τους κανονισμούς προστασίας δεδομένων αποτελεί ζωτικής σημασίας στοιχείο για τη διασφάλιση της ιδιωτικότητας, της εμπιστοσύνης και της ασφάλειας των προσωπικών δεδομένων σε μια παγκοσμιοποιημένη και ψηφιακά διασυνδεδεμένη κοινωνία. Οι κανονισμοί περί απορρήτου δεδομένων έχουν περιορίσει τον όγκο των δεδομένων καταναλωτών που μπορούν να συλλεχθούν και αύξησαν τον έλεγχο που έχουν τα υποκείμενα των δεδομένων σχετικά με τον τρόπο χρήσης και αποθήκευσης των δεδομένων τους. Αντί να βασίζονται σε τρίτους για την ελαχιστοποίηση των κινδύνων δεδομένων, ένας αυξανόμενος αριθμός επιχειρήσεων επιλέγει να διατηρήσει όλες τις δραστηριότητές τους στο εσωτερικό. Ένα σημαντικό μέρος των προϋπολογισμών διατίθεται πλέον για την πρόληψη του εγκλήματος στον κυβερνοχώρο και έχουν δημιουργηθεί νέες θέσεις για την ασφάλεια των δεδομένων. Συμπερασματικά, η παρούσα έρευνα διαπίστωσε ότι οι επιχειρηματίες γνώριζαν ικανοποιητικά το Γενικό Κανόνα για την Προστασία των Δεδομένων, αλλά υπήρχε μέτρια συμμόρφωση και μέτριες αντιλήψεις για αυτόν. Επιπλέον, ο βαθμός συμμόρφωσης και οι αντιλήψεις για τον Γενικό Κανόνα για την Προστασία των Δεδομένων δεν σχετίζονταν με τα δημογραφικά χαρακτηριστικά των επιχειρηματιών, ούτε με τα στοιχεία της επιχείρησης. Προτείνεται η εις βάθος διερεύνηση, με τη χρήση συνεντεύξεων, των αντιλήψεων των επιχειρηματιών αναφορικά με τα πλεονεκτήματα, τα μειονεκτήματα και τις προκλήσεις του

Γενικού Κανονισμού για την Προστασία των Δεδομένων. Επίσης, είναι σημαντικό να διερευνηθεί ο βαθμός συμμόρφωσης στο Γενικό Κανονισμό για την Προστασία των Δεδομένων, με δείγμα επιχειρήσεις σε πανελλαδικό επίπεδο.

Βιβλιογραφία

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.

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

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

Alhadeff, J., Van Alsenoy, B., & Dumortier, J. (2012). The accountability principle in data protection regulation: origin, development and future directions. In *Managing privacy through accountability* (pp. 49-82). London: Palgrave Macmillan UK.

Anthonysamy, P., Rashid, A., & Chitchyan, R. (2017). Privacy requirements: present & future. In *2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS)* (pp. 13-22). IEEE.

Apthorpe, N., Varghese, S., & Feamster, N. (2019). Evaluating the Contextual Integrity of Privacy Regulation: Parents'{IoT} Toy Privacy Norms Versus {COPPA}. In *28th USENIX security symposium (USENIX security 19)* (pp. 123-140).

Aslam, U., Kiani, N., & Chian, Z. (2023). Legal Implications of Strategic Marketing: Navigating Compliance in a Digital Age.

Augustine, D. (2019). Working around the law: Navigating legal barriers to employment during reentry. *Law & Social Inquiry*, *44*(3), 726-751.

Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods*. Oxford university press.

Boban, M. (2016). ePrivacy and new European Data Protection Regime. *Economic and Social Development: Book of Proceedings*, 152.

Boyne, S. M. (2018). Data protection in the United States. *The American Journal of Comparative Law*, *66*(suppl_1), 299-343.

Braun, A., & Garriga, G. (2017). Consumer journey analytics in the context of data privacy and ethics. In *Digital marketplaces unleashed* (pp. 663-674). Berlin, Heidelberg: Springer Berlin Heidelberg.

Brodin, M. (2019). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research*, 4(2), 1-22.

Burgess, M. (2020). What is GDPR? The summary guide to GDPR compliance in the UK. *Wired UK*, *21*. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Butarbutar, R. (2020). Initiating new regulations on personal data protection: Challenges for personal data protection in indonesia. In *3rd International Conference on Law and Governance (ICLAVE 2019)* (pp. 154-163). Atlantis Press.

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200.

Canedo, E. D., Ribeiro, V. C., Alarcão, A. P. D. A., Chaves, L. A. C., Reed, J. N., Mendonça, F. L. L., & de Sousa Jr, R. T. (2021). Challenges Regarding the Compliance with the General Data Protection Law by Brazilian Organizations: A Survey. In *Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part III 21* (pp. 438-453). Springer International Publishing.

Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law & Security Review*, *32*(3), 462-473.

Cate, F. H. (2016). The failure of fair information practice principles. In *Consumer Protection in the Age of the'Information Economy'* (pp. 341-377). Routledge.

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century.

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience*, *11*.

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, *187*(1), 199-224.

Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent. *Sensors*, *22*(7), 2763.

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157-170.

Crutzen, R., Ygram Peters, G. J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, *34*(11), 1347-1357.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*.

de Carvalho, R. M., Del Prete, C., Martin, Y. S., Araujo Rivero, R. M., Önen, M., Schiavo, F. P., ... & Koukovini, M. N. (2020). Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. *SN Computer Science*, *1*, 1-16.

De Guise, P. (2017). *Data protection: Ensuring data availability*. Auerbach Publications.

Del Vecchio, P., Di Minin, A., Messeni Petruzzelli, A., Panniello, U., & Pirri, S. (2018). Big data for open innovation in SMEs and large corporations: Trends, opportunities, and challenges. *Creative Innovations in Management, 27*, 6–22.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk'in the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105342.

Demirer, M., Hernández, D. J., Li, D., & Peng, S. (2023). *Data, privacy laws, and firm production: Evidence from GDPR.* Retrieved from https://www.diegojimenezh.com/assets/pdf/Demirer_et_al2023_Privacy.pdf [accessed 20/1/2024].

Diaz Diaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture*, *1*(1), 206-239.

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

Dove, E. S., & Phillips, M. (2015). Privacy law, data sharing policies, and medical data: a comparative perspective. *Medical data privacy handbook*, 639-678.

Duncan, R. A. K., & Whittington, M. (2016). Enhancing cloud security and privacy: The power and the weakness of the audit trail. *Cloud Computing 2016*.

Eling, M., & Loperfido, N. (2017). Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: mathematics and economics*, *75*, 126-136.

EPSU. (2018). General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October*, *24*(1).

Eriksson, P., & Kovalainen, A. (2015). *Qualitative methods in business research: A practical guide to social research*. Sage.

Ezor, J. I. (2012). Privacy and data protection in business: Laws and practices. *J. Ezor, Privacy and Data Protection in Business: Laws and Practices*, 1-66.

Fernando, Y., Chidambaram, R. R., & Wahyuni-TD, I. S. (2018). The impact of Big Data analytics and data security practices on service supply chain performance. *Benchmarking: An International Journal*, *25*(9), 4009-4034.

Ferris, J. L. (2017). Data privacy and protection in the agriculture industry: Is federal regulation necessary. *Minn. JL Sci. & Tech.*, *18*, 309.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Security Review*, *32*(4), 577-586.

Foulsham, M. (2019). Living with the new general data protection regulation (GDPR). *Financial Compliance: Issues, Concerns and Future Directions*, 113-136.

Frik, A., & Mittone, L. (2019). Factors influencing the perception of website privacy trustworthiness and users' purchasing intentions: The behavioral economics perspective. *Journal of theoretical and applied electronic commerce research*, *14*(3), 89-125.

Gao, Y. L., Zhang, L., & Wei, W. (2021). The effect of perceived error stability, brand perception, and relationship norms on consumer reaction to data breaches. *International Journal of Hospitality Management*, *94*, 102802.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279-288.

Georgiadis, G., & Poels, G. (2021). Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study. *Information Systems and e-Business Management*, *19*, 313-362.

Georgiopoulou, Z., Makri, E. L., & Lambrinoudakis, C. (2020). GDPR compliance: proposed technical and organizational measures for cloud provider. *Information & Computer Security*, *28*(5), 665-680.

Grundstrom, C., Väyrynen, K., Iivari, N., & Isomursu, M. (2019). Making sense of the general data protection regulation—four categories of personal data access challenges.
Grundstrom, C., Väyrynen, K., Iivari, N., & Isomursu, M. (2019). Making sense of the general data protection regulation—four categories of personal data access challenges.

Gurkaynak, G., Yilmaz, I., & Taskiran, N. P. (2014). Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer law & security review*, *30*(2), 179-189.

Guseva, O.Y., Kazarova, I.O., Dumanska, I.Y., Gorodetskyy, M.A., Melnitchuk, L.V., & Saienko, V. (2022). Personal Data Protection Policy Impact on the Company Development. *WSEAS Transactions on Environment and Development*, *18*, 232-246.

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, *151*, 1004-1009.

Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, 1687.

Hendrickx, F. (2022). *Protection of workers' personal data: General principles* (No. 62). ILO Working Paper.

Hjerppe, K., Ruohonen, J., & Leppänen, V. (2019). The general data protection regulation: requirements, architectures, and constraints. In *2019 IEEE 27th International Requirements Engineering Conference (RE)* (pp. 265-275). IEEE.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Frontiers in Computer Science*, *2*, 36.

Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *Eur. Data Prot. L. Rev.*, *4*, 168.

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, *28*(2), 275-301.

Kasirzadeh, A., & Clifford, D. (2021). Fairness and data protection impact assessments. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 146-153).

Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

Koski, H., & Valmari, N. (2020). *Short-term Impacts of the GDPR on Firm Performance*. Retrieved from https://www.econstor.eu/bitstream/10419/237362/1/ETLA-Working-Papers-77.pdf [accessed 21/1/2024].

Koutroumpis, P., Ravasan, F., & Tarannum, T. (2022). *(Under) Investment in Cyber Skills and Data Protection Enforcement: Evidence from Activity Logs of the UK Information Commissioner's Office*. Retrieved from https://ssrn.com/abstract=4179601 [accessed 21/1/2024].

Kulkarni, V., Sunkle, S., Kholkar, D., Roychoudhury, S., Kumar, R., & Raghunandan, M. (2021). Toward automated regulatory compliance. *CSI Transactions on ICT*, *9*, 95-104.

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. *Update of Selected Articles (May 4, 2021)*.

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B., & Lynskey, O. (2015). Risk management in data protection. *International Data Privacy Law*, *5*(2), 95-98.

Layton, R. (2017). How the GDPR compares to best practices for privacy, accountability and trust. *Accountability and Trust (March 31, 2017)*.

Li, C. Y. (2015). Switching barriers and customer retention: Why customers dissatisfied with online service recovery remain loyal. *Journal of Service Theory and Practice*, *25*(4), 370-393.

Li, S. C., Chen, Y. W., & Huang, Y. (2021). Examining compliance with personal data protection regulations in interorganizational data analysis. *Sustainability*, *13*(20), 11459.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*, 106868.

Liu, C. T., Guo, Y. M., & Lee, C. H. (2011). The effects of relationship quality and switching barriers on customer loyalty. *International Journal of Information Management*, *31*(1), 71-79.

London Economics. (2013). *Implications of the European Commission's proposal for a general data protection regulation for business*. Retrieved from https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf [accessed 21/1/2024].

Maex, S. A. (2022). *Modern privacy regulation, internal information quality, and operating efficiency: Evidence from the General Data Protection Regulation*. Retrieved from https://scholarshare.temple.edu/handle/20.500.12613/8053 [accessed 21/1/2024].

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., ... & Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *computer law & security review*, *33*(4), 458-469.

Mantelero, A. (2013). Competitive value of data protection: the impact of data protection regulation on online behaviour. *International Data Privacy Law*, *3*(4), 229-238.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer law & security review*, *32*(2), 238-255.

Marikyan, D., Papagiannidis, S., Rana, O.F., & Ranjan, R. (2022). General data protection regulation: a study on attitude and emotional empowerment. *Behaviour & Information Technology*, https://doi.org/10.1080/0144929X.2023.2285341

Marr, B. (2015). *Big Data: Using SMART big data, analytics and metrics to make better decisions and improve performance*. John Wiley & Sons.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58.

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information systems frontiers*, *21*, 1307-1324.

Meszaros, J., & Ho, C. H. (2021). AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?. *Computer Law & Security Review*, *41*, 105532.

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision support systems*, *54*(1), 198-205.

Mikkonen, T. (2014). Perceptions of controllers on EU data protection reform: A Finnish perspective. *Computer Law & Security Review, 30* (2), 190-195.

Mizarhi-Borohovich, I., Newman, A., & Sivan-Sevilla, I. (2024). The civic transformation of data privacy implementation in Europe. *West European Politics*, *47*(3), 671-700.

Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR compliance through the lens of privacy policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare: VLDB 2019 Workshops, Poly and DMAH, Los Angeles, CA, USA, August 30, 2019, Revised Selected Papers 5* (pp. 82-95). Springer International Publishing.

Mondschein, C. F., & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a research context. *Fundamentals of clinical data science*, 55-71.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96-105.

Mubarak Alharbi, I., Zyngier, S., & Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management*, *26*(6), 702-718.

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, *34*(6), 1232-1246.

No, E. (2018). General data protection regulation (gdpr).

Okeke, R. I., Shah, M. H., & Ahmed, R. (2013). Issues of privacy and trust in e-commerce: Exploring customers' perspective. *Journal of Basic and Applied Scientific Research*, *3*(3), 571-577.

Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security*, *117*, 102697.

Palmer, D. (2019). What is GDPR? Everything you need to know about the new general data protection regulations. *ZDNet.* *https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/*

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575-582.

Piwik. (2023). *Five years into GDPR: How EU companies balance compliance and effective marketing.* Retrieved from https://piwik.pro/report/five-years-into-gdpr/ [accessed 21/1/2024].

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299-1323.

Ruivo, P., Santos, V., & Oliveira, T. (2014). Data protection in services and support roles–a qualitative research amongst ICT professionals. *Procedia Technology*, *16*, 710-717.

Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Fla. L. Rev.*, *71*, 365.

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, *2*(1), 15-28.

Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*, *2*, e4.

Stuurman, K., & Kamara, I. (2016). IoT Standardization-The Approach in the Field of Data Protection as a Model for Ensuring Compliance of IoT Applications?. In *2016 IEEE 4th International Conference on Future internet of things and Cloud Workshops (FiCloudW)* (pp. 336-341). IEEE.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Susanto, H., Fang Yie, L., Mohiddin, F., Rahman Setiawan, A. A., Haghi, P. K., & Setiana, D. (2021). Revealing social media phenomenon in time of COVID-19 pandemic for boosting start-up businesses through digital ecosystem. *Applied system innovation*, *4*(1), 6.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, *28*(3), 257-274.

Taherdoost, H. (2023). Legal, Regulatory, and Ethical Considerations in E-Business. In *E-Business Essentials: Building a Successful Online Enterprise* (pp. 379-402). Cham: Springer Nature Switzerland.

Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, *91*, 101469.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Thüsing, G., & Traut, J. (2013). The reform of European data protection law: harmonisation at last? *Intereconomics, 48* (5), 271–276.

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

Torra, V., & Navarro-Arribas, G. (2016). Big data privacy and anonymization. *Privacy and Identity Management. Facing up to Next Steps: 11th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2. 2 International Summer School, Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers 11*, 15-26.

TRUSTe. (2015). *Preparing for the EU General Data Protection Regulation*. Retrieved from https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf [accessed 22/1/2024].

van Deenen, B., Nauts, P., Trietsch, R., & Voorn, B. (2022). Towards Privacy by Design for Data with STRM privacy. *Data Engineering*, 62.

Van Kleek, M., & OHara, K. (2014). The future of social is personal: The potential of the personal data store. In *Social collective intelligence: Combining the powers of humans and machines to build a smarter society* (pp. 125-158). Cham: Springer International Publishing.

Viljoen, S. (2021). A relational theory of data governance. *Yale LJ*, *131*, 573.

von Grafenstein, M., Jakobi, T., & Stevens, G. (2022). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. *Computer Law & Security Review*, *46*, 105722.

Wang, S., & Wang, H. (2020). Big data for small and medium-sized enterprises (SME): A knowledge management model. *Journal of Knowledge Management*, *24*, 881–897. Bertino, E. (2016). Introduction to data security and privacy. *Data Science and Engineering*, *1*(3), 125-126.

Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *International Journal of Information Management*, *50*, 387-394.

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

Xu, H. (2011). Consumer responses to the introduction of privacy protection measures: an exploratory research framework. In *E-Business Applications for Product Development and Competitive Growth: Emerging Technologies* (pp. 161-185). IGI global.

Zarei, B., Nasseri, H., & Tajeddin, M. (2011). Best practice network business model for internationalization of small and medium enterprises. *Journal of International Entrepreneurship, 9*, 299-315.

Δαφέρμος, Β. (2011). *Κοινωνική στατιστική και μεθοδολογία έρευνας με το SPSS*. Θεσσαλονίκη: Εκδόσεις Ζήτη.

Παράρτημα

Ερωτηματολόγιο

Α. Δημογραφικά χαρακτηριστικά

Φύλο

- Άνδρας
- Γυναίκα

Ηλικία

- Έως 30 ετών
- 31-45 ετών
- 46-55 ετών
- 56-65 ετών

Μορφωτικό επίπεδο

- Απόφοιτος γυμνασίου
- Απόφοιτος λυκείου
- Απόφοιτος ΑΕΙ/ΤΕΙ
- Κάτοχος μεταπτυχιακού
- Κάτοχος διδακτορικού

Θέση στην επιχείρηση

- Ιδιοκτήτης

- Διευθυντής
- Στέλεχος
- Μέτοχος

Είδος επιχείρησης

- Ατομική εταιρεία
- Ομόρρυθμη εταιρεία
- Ετερόρρυθμη εταιρεία
- Μονοπρόσωπη περιορισμένης ευθύνης εταιρεία
- Περιορισμένης ευθύνης εταιρεία
- Ιδιωτική κεφαλαιουχική εταιρεία
- Ανώνυμη εταιρεία

Μέγεθος επιχείρησης

- Πολύ μικρή (0-10 άτομα)
- Μικρή (μέχρι 50 άτομα)
- Μεσαία (μέχρι 250 άτομα)
- Μεγάλη (πάνω από 250 άτομα)

Τομέας δραστηριοποίησης επιχείρησης

- Κατασκευές
- Μεσιτικά
- Μεταποίηση
- Εμπόριο
- Εφοδιαστική αλυσίδα και μεταφορές
- Τουρισμός
- Χρηματοοικονομικές υπηρεσίες
- Πληροφορική και επικοινωνίες

Β. Γνώση και συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων

Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων;

- Καθόλου
- Λίγο
- Μέτρια
- Πολύ
- Πάρα πολύ

Έχει γίνει εκπαίδευση των εργαζομένων σε θέματα σχετικά με το Γενικό Κανονισμό για την Προστασία των Δεδομένων;

- Ναι
- Όχι

Διατηρούνται τα προσωπικά δεδομένα πελατών, συνεργατών, προμηθευτών και υπαλλήλων (δηλ. ονοματεπώνυμο, διεύθυνση, κινητό τηλέφωνο, email κλπ);

- Ναι
- Όχι
- Ορισμένες φορές μόνο

Διαμοιράζονται τα προσωπικά δεδομένα που διατηρούνται με άλλους οργανισμούς και επιχειρήσεις;

- Ναι
- Όχι
- Ορισμένες φορές μόνο

Γίνεται χρήση των προσωπικών δεδομένων που διατηρούνται για προωθητικές ενέργειες πωλήσεων;

- Ναι
- Όχι
- Ορισμένες φορές μόνο

Όταν αποστέλλονται email ή SMS στα άτομα των οποίων διατηρείτε τα προσωπικά τους δεδομένα, δίνεται η δυνατότητα διακοπής της επικοινωνίας (διαγραφή) με κατανοητό και απλό τρόπο;

- Ναι
- Όχι
- Εν μέρει

Τα φυσικά πρόσωπα γνωρίζουν ότι έχετε τα προσωπικά τους δεδομένα και τον λόγο και τον τρόπο χρήσης τους;

- Ναι
- Όχι
- Ορισμένες φορές μόνο

Τα προσωπικά δεδομένα διατηρούνται για όσο διάστημα χρειάζεται;

- Ναι
- Όχι
- Εν μέρει

Τα προσωπικά δεδομένα διατηρούνται ακριβή και ενημερωμένα;

- Ναι
- Όχι
- Εν μέρει

Τα προσωπικά δεδομένα διατηρούνται ασφαλή;

- Ναι
- Όχι
- Εν μέρει

Γνωρίζετε τα δικαιώματα των ατόμων των οποίων διατηρείτε και αποθηκεύετε τα προσωπικά τους δεδομένα;

- Ναι
- Όχι
- Εν μέρει

Ποια από τα παρακάτω δικαιώματα μπορούν να εξασκήσουν τα άτομα των οποίων διατηρείτε και αποθηκεύτε τα προσωπικά τους δεδομένα;

- Πρόσβαση ή λήψη αντιγράφου
- Ενημέρωση δεδομένων
- Διόρθωση δεδομένων
- Διαγραφή δεδομένων
- Περιορισμός επεξεργασίας
- Μεταφορά δεδομένων
- Υποβολή ένστασης

Στην ιστοσελίδα της επιχείρησης περιγράφεται λεπτομερώς η πολική απορρήτου προσωπικών δεδομένων της επιχείρησης;

- Ναι
- Όχι

Γ. Αντιλήψεις για το Γενικό Κανονισμό για την Προστασία των Δεδομένων

Σε ποιο βαθμό θεωρείτε εύκολη την προσαρμογή στο Γενικό Κανονισμό για την Προστασία των Δεδομένων;

- Καθόλου
- Λίγο
- Μέτρια
- Πολύ
- Πάρα πολύ

Πόσο δύσκολη θεωρείτε την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων;

- Καθόλου
- Λίγο
- Μέτρια
- Πολύ
- Πάρα πολύ

Πόσο υψηλό θεωρείτε το κόστος της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων;

- Καθόλου
- Λίγο
- Μέτρια
- Πολύ
- Πάρα πολύ

Σε ποιο βαθμό πιστεύετε ότι η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων μειώνει τα έσοδα της επιχείρησης;

- Καθόλου
- Λίγο
- Μέτρια
- Πολύ
- Πάρα πολύ