

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
ΚΟΙΝΩΝΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Μεταπτυχιακή Διατριβή



**Γενικός Κανονισμός Προστασίας Δεδομένων
(GDPR), Προστασία της Ιδιωτικότητας και
Δικαιώματα των χρηστών.**

Αθανάσιος Φονταράς

**Επιβλέπουσα Καθηγήτρια
Μαρία Σιδερή**

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

**Μεταπτυχιακό Πρόγραμμα Σπουδών
ΚΟΙΝΩΝΙΚΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

Μεταπτυχιακή Διατριβή

**Γενικός Κανονισμός Προστασίας Δεδομένων
(GDPR), Προστασία της Ιδιωτικότητας και
Δικαιώματα των χρηστών.**

Αθανάσιος Φονταράς

**Επιβλέπουσα Καθηγήτρια
Μαρία Σιδερή**

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Κοινωνικά Πληροφοριακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2019

Περίληψη

Η παρούσα διατριβή στοχεύει στη διερεύνηση της γνώσης ομάδας ενηλίκων χρηστών του Διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης (ΜΚΔ) σχετικά με τις ρυθμίσεις που φέρνει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) στο θέμα της συλλογής και διαχείρισης προσωπικών τους δεδομένων από οργανισμούς, εταιρείες ή παρόχους και των δικαιωμάτων που οι χρήστες έχουν. Συγκεκριμένα, στόχος είναι να εξεταστεί αν οι χρήστες γνωρίζουν και σε ποιο βαθμό τη νέα νομοθεσία και κατανοούν τις προβλέψεις - δικαιώματα που θεσπίζονται γι' αυτούς. Σε δεύτερο επίπεδο, καθώς η γνώση δυνητικά επιδρά στη στάση και τη συμπεριφορά, επιχειρείται η καταγραφή στάσεων και συμπεριφορών των χρηστών στο θέμα της προστασίας της ιδιωτικότητάς τους. Για την εκπόνηση της διατριβής πραγματοποιήθηκε ενδελεχής μελέτη του ΓΚΠΔ για την αποτύπωση των ρυθμίσεων του σε σχέση με τη διαχείριση και προστασία των δεδομένων των χρηστών σε συνδυασμό με προηγούμενες νομοθετικές ρυθμίσεις και υλοποιήθηκε ποσοτική έρευνα με τη χρήση ερωτηματολογίου για τη διερεύνηση της σχετικής γνώσης των χρηστών, του βαθμού συνείδησης ιδιωτικότητας και των στάσεων και συμπεριφορών τους για την προστασία της ιδιωτικότητας και των προσωπικών τους δεδομένων.

Η έρευνα καταδεικνύει ότι δεν υπάρχει υψηλός βαθμός γνώσης για όλα τα δικαιώματα που έχουν οι χρήστες ή για τις προϋποθέσεις άσκησης αυτών. Για παράδειγμα γνωρίζουν πως η συγκατάθεσή τους απαιτείται για την επεξεργασία των δεδομένων τους, αλλά δεν γνωρίζουν καλά το δικαίωμα στη φορητότητα των δεδομένων τους. Επιπλέον, τα αποτελέσματα της έρευνας δείχνουν ότι αν και τα υποκείμενα των δεδομένων ανησυχούν σε υψηλό βαθμό για το ποιος και πώς διαχειρίζεται τα δεδομένα τους και αγωνιούν για τους κινδύνους από την απώλεια ή κλοπή αυτών, ωστόσο σε υψηλό ποσοστό διαβάζουν μερικώς τις πολιτικές απορρήτου και δεν είναι βέβαιοι που πρέπει να απευθυνθούν σε περίπτωση παραβίασης των προσωπικών τους δεδομένων.

Λέξεις κλειδιά: Γενικός Κανονισμός Προστασίας Δεδομένων, υποκείμενα των δεδομένων, δικαιώματα, προσωπικά δεδομένα, ιδιωτικότητα

Abstract

This dissertation aims at exploring the knowledge of an adult group of Internet and Social Media users regarding the General Data Protection Regulation (GDPR) with specific reference to the provisions about the collection and management of personal data by organizations, companies or providers as well as about users' rights. In particular, it aims to investigate whether users are familiar with the new legislation and to what extent, and whether they understand the rights established for them. Moreover, as knowledge potentially affects attitudes and behaviors, the dissertation attempts to record users' attitudes and behaviors regarding their privacy protection. The following steps were followed during the dissertation: a) study and mapping of the GDPR regulations for the management and protection of users data in correlation with previous legislation and b) implementation of quantitative research using a questionnaire for the investigation of the users' knowledge regarding GDPR, the level of their privacy awareness and their attitudes and behaviors towards privacy and data protection.

Findings don't record users' high level of knowledge regarding all their rights nor regarding the conditions for exercising them. For example, users acknowledge that their consent is required for data processing, but they are not sufficiently aware of the right to portability of their data. In addition, research shows that although data subjects are highly concerned about who manage their data and how, and worry about the risks resulting from their data loss or theft, they still partially read privacy policies and are not sure to whom they should address in case of violation of their personal data.

Keywords: General Data Protection Regulation, data subjects, rights, personal data, privacy

Ευχαριστίες

Η εκπόνηση της παρούσας μεταπτυχιακής διατριβής πραγματοποιήθηκε υπό την επίβλεψη της κυρίας Μαρίας Σιδερέ, καθηγήτρια στο Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας του Πανεπιστημίου Αιγαίου. Την ευχαριστώ θερμά για τη συνεχή καθοδήγηση, την αμέριστη υποστήριξη, τις ουσιώδεις συμβουλές, καθώς επίσης και την αδιάκοπη συμπαράσταση και ενθάρρυνση που μου παρείχε σε όλο αυτό το χρονικό διάστημα.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου για την κατανόηση και την υποστήριξή τους, καθώς και τους φίλους οι οποίοι προσέφεραν με το δικό τους τρόπο στην προσπάθεια ολοκλήρωσης της παρούσας διπλωματικής.

Στον γιό μου Κωνσταντίνο.

Περιεχόμενα

Εισαγωγή.....	1
Κεφάλαιο 1	6
Ο νέος Ευρωπαϊκός Κανονισμός.....	6
1.1 Υποχρεώσεις στη διαδικασία επεξεργασίας Προσωπικών Δεδομένων	8
1.2. Υπεύθυνος προστασίας δεδομένων (Data Protection Officer)	10
1.3 Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (Data Protection Impact Assessment).....	12
1.4 Τα δικαιώματα των υποκειμένων των δεδομένων.....	13
1.5. Εποπτική Αρχή.....	20
Κεφάλαιο 2	21
Η Ελληνική Νομοθεσία	21
2.1. Ο Νόμος 2472/97.....	23
2.2. Τα δικαιώματα των υποκειμένων	26
Κεφάλαιο 3	28
Η Ιδιωτικότητα στην Κοινωνία της Πληροφορίας.....	28
3.1 Προκλήσεις στην προστασία της ιδιωτικότητας.....	29
3.2 Οι ανησυχίες ιδιωτικότητας των χρηστών.....	31
3.3 Οι απόψεις των υποκειμένων των δεδομένων για τη νομοθεσία και το ρόλο της.....	33
Κεφάλαιο 4	35
Μεθοδολογία Έρευνας.....	35
4.1 Δήλωση σκοπού έρευνας.....	36
4.2 Οργάνωση Ερευνητικής Διαδικασίας.....	37
4.2.1. Επιλογή δείγματος.....	37
4.2.2. Ερευνητικό Εργαλείο.....	37
Κεφάλαιο 5	40
Αποτελέσματα Έρευνας.....	40
5.1. Ενότητα Α «Γενικός Κανονισμός Προστασίας Δεδομένων».....	41

5.2. Ενότητα Β «Τα δικαιώματα των υποκειμένων των δεδομένων».....	43
5.3. Ενότητα Γ, υποενότητα Γ.1 «Έλεγχος Προσωπικών Δεδομένων και Κίνδυνοι».....	54
5.4. Ενότητα Γ, υποενότητα Γ.2 «Προστασία Προσωπικών Δεδομένων».....	61
Κεφάλαιο 6	73
Συμπεράσματα.....	73
Βιβλιογραφικές Αναφορές.....	82
Παράρτημα Α	87
Σύγκριση Κανονισμού 2016/679/ΕΕ με Οδηγία 95/46/ΕΕ	87
Παράρτημα Β	92
Ερωτηματολόγιο	92
Παράρτημα Γ.....	101
Αποτελέσματα.....	101

Εισαγωγή

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) (Ευρ. Κοινοβούλιο, 679/2016) ψηφίσθηκε στις 16 Απριλίου 2016 από το Ευρωπαϊκό Κοινοβούλιο, αντικαθιστώντας την οδηγία 95/46/ΕΚ για την Προστασία Προσωπικών Δεδομένων. Τέθηκε σε ισχύ στις 5 Μαΐου 2016 με μεταβατική περίοδο 2 ετών και εφαρμόστηκε ως νομοθέτημα άμεσης εφαρμογής σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης, στις 25 Μαΐου 2018. Ο Κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης (Ε.Ε), δηλαδή για την εφαρμογή του δεν απαιτείται ειδική προσαρμογή της εθνικής νομοθεσίας (άρθρο 83, 679/2016 ΕΕ). Μέχρι σήμερα, με εξαίρεση 5 χώρες (Βουλγαρία, Ελλάδα, Σερβία, Πορτογαλία και Τσεχία), 23 κράτη-μέλη της Ε.Ε. έχουν προσαρμόσει την εθνική τους νομοθεσία.

Αν και ο ΓΚΠΔ δεν αποτελεί, σε ευρωπαϊκό επίπεδο, την πρώτη προσπάθεια νομικής κατοχύρωσης και διασφάλισης των προσωπικών δεδομένων των υποκειμένων, καθώς έχουν ήδη προηγηθεί ευρωπαϊκές οδηγίες, αλλά και σχετικές εθνικές νομικές ρυθμίσεις, ο νέος Κανονισμός εισάγει ένα αυστηρότερο πλαίσιο στη διαχείριση των δεδομένων, ενισχύει τα δικαιώματα των υποκειμένων και αυξάνει τις υποχρεώσεις των διαχειριστών δεδομένων, ενώ διευρύνει και το πεδίο εφαρμογής του, αφού απευθύνεται σε κάθε επιχείρηση ή οργανισμό που διαχειρίζεται δεδομένα πολιτών της Ένωσης, ανεξαρτήτως αν βρίσκεται εντός της εδαφικής επικράτειάς της. Ενώ, λοιπόν, οι κανόνες είναι αυστηρότεροι τώρα, οι βασικές αρχές παραμένουν εν πολλοίς οι ίδιες εδώ και πολλά χρόνια. Υπό αυτή την έννοια, ο ΓΚΠΔ αφορά περισσότερο την ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων και τις διαδικασίες ελέγχου της συμμόρφωσης με τη νομοθεσία, παρά την οικοδόμηση κάτι νέου από το μηδέν. Η εφαρμογή του ΓΚΠΣ αφορά σε κάθε δραστηριότητα αυτοματοποιημένης ή μη επεξεργασίας προσωπικών δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Σύμφωνα με τον ΓΚΠΔ, ως «δεδομένα προσωπικού χαρακτήρα» ορίζεται:

κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του

οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου (Άρθ. 4, 679/2016 ΕΕ).

Συνοπτικά, οι αρχές του Κανονισμού καθορίζουν πως τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε διαφανή και ασφαλή επεξεργασία (προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, φθορά ή καταστροφή), να συλλέγονται για συγκεκριμένους και σύννομους σκοπούς, να περιορίζονται στο αναγκαίο, να είναι ακριβή και να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση προσώπων μόνο για το αναγκαίο χρονικό διάστημα. Εξάιρεση αποτελούν οι περιπτώσεις που η επεξεργασία προσωπικών δεδομένων πραγματοποιείται για την προστασία του δημόσιου συμφέροντος (π.χ. υγειονομική προστασία) ή για επιστημονικούς και στατιστικούς σκοπούς. Επιπλέον, σύμφωνα με τον Κανονισμό, τα υποκείμενα των δεδομένων ισχυροποιούν τα δικαιώματά τους ή αποκτούν νέα, μεταξύ άλλων αυτών της φορητότητας των δεδομένων. Απαγορεύεται δε η χρήση προσωπικών δεδομένων χωρίς την ελεύθερη συγκατάθεση των υποκειμένων, ειδικά όταν πρόκειται για ευαίσθητη κατηγορία δεδομένων, και καθορίζεται πως η συγκατάθεση μπορεί να ανακληθεί ελεύθερα οποιαδήποτε στιγμή. Περαιτέρω, στον Κανονισμό εισάγεται ρύθμιση για το θέμα της κατάρτισης προφίλ και για τα δικαιώματα των υποκειμένων έναντι της απολύτως αυτοματοποιημένης λήψης αποφάσεων και των συνέπειών της. Τέλος, δίνεται ιδιαίτερη βαρύτητα στην ασφάλεια των προσωπικών δεδομένων, ώστε να προστατεύονται στο μέγιστο τα ατομικά δικαιώματα.

Ο Κανονισμός στοχεύει τόσο στην θέσπιση ενός ενιαίου πλαισίου προστασίας των προσωπικών δεδομένων σε όλη την Ένωση, όσο και στην διασφάλιση της ελεύθερης διασυνοριακής διακίνησης δεδομένων. Πώς, όμως, προέκυψε η ανάγκη για μια τέτοια νομική ρύθμιση και εφαρμογή ενός καθολικά ευρωπαϊκού νόμου;

Οι ραγδαίες τεχνολογικές εξελίξεις, η παγκοσμιοποίηση της χρήσης του διαδικτύου (πάνω από 250 εκατομμύρια οι χρήστες στην Ευρώπη), η συνεχώς αυξανόμενη χρήση των κινητών συσκευών (π.χ. Smartphones), τα μέσα κοινωνικής δικτύωσης, οι υπηρεσίες

cloud είναι μια καθημερινή πραγματικότητα στις ιδιωτικές και επαγγελματικές δραστηριότητες των πολιτών, οι οποίες οδηγούν στη δημιουργία ενός πολύ μεγάλου όγκου προσωπικών δεδομένων, τα οποία διαβιβάζονται και ανταλλάσσονται μεταξύ διαφόρων φορέων και κρατών εντός και εκτός της Ευρωπαϊκής Ένωσης. Δεν είναι τυχαίο, άλλωστε, ότι τα δεδομένα αναφέρονται πλέον ως η πολυτιμότερη πηγή της παγκόσμιας οικονομίας και όχι το πετρέλαιο (Economist, 2017). Εταιρείες κολοσσοί με παγκόσμια παρουσία, όπως είναι το Facebook, αντιμετώπισαν σοβαρές υποθέσεις παραβίασης ή διαρροής προσωπικών δεδομένων. Η περίπτωση της σύνδεσης μεταξύ του Facebook και της εταιρείας Cambridge Analytica (Facebook–Cambridge Analytica data scandal) είναι μια από τις πιο πρόσφατες. Αποτέλεσμα ήταν όχι μόνο η απώλεια δεδομένων των πολιτών, αλλά και η ζημιά στο σημαντικότερο περιουσιακό στοιχείο μιας εταιρείας: την καλή φήμη και αξιοπιστία της.

Η Ευρωπαϊκή Επιτροπή αντιλαμβανόμενη την ανάγκη να ανταποκριθεί στις προκλήσεις της Κοινωνίας της Πληροφορίας και να διασφαλίσει μια οργανωμένη, συνολική και ενιαία διαδικασία συμμόρφωσης των κρατών μελών στο θέμα της προστασίας των προσωπικών δεδομένων, κατέληξε στην σύνταξη και ψήφιση του Κανονισμού Προστασίας Δεδομένων για όλα τα κράτη μέλη της ΕΕ. Ο τρόπος που η συμμόρφωση σχεδιάστηκε, ανταποκρίνεται στην ψηφιακή πραγματικότητα φέρνοντας κανόνες και υποχρεώσεις που συμβαδίζουν με την ταχύτητα της διαδικτυακής εποχής. Στόχος του Κανονισμού, λοιπόν, είναι να διασφαλίσει ότι η προστασία των δεδομένων, που αποτελεί θεμελιώδες ανθρώπινο δικαίωμα, θα ρυθμίζεται με συνέπεια σε όλη την Ευρώπη. Ο πυρήνας του ΓΚΠΔ απαρτίζεται από ένα σύνολο κανόνων που έχουν ως τελικό σκοπό να παράσχουν στους πολίτες μεγαλύτερο έλεγχο πάνω στα προσωπικά τους δεδομένα. Πρακτικά, ο ΓΚΠΔ απλοποιεί και ενοποιεί το νομικό περιβάλλον, ώστε τόσο οι πολίτες όσο και οι επιχειρήσεις να μπορούν να ωφεληθούν από την ψηφιακή οικονομία, ανεξάρτητα σε ποια χώρα της Ε.Ε. δραστηριοποιούνται.

Μέσα στο πλαίσιο αυτό της εντεινόμενης μέριμνας για την νομική προστασία της ιδιωτικότητας των πολιτών, διαπιστώνεται σε αρκετές περιπτώσεις ότι οι ίδιοι οι πολίτες λανθασμένα θεωρούν πως έχουν γνώση της νομοθεσίας και των ενεργειών στις οποίες πρέπει να προβούν, σε περίπτωση που διαπιστώσουν περιστατικό παραβίασης των δεδομένων τους, ενώ επιπλέον, σε άλλες περιπτώσεις, εκφράζουν την εμπιστοσύνη τους στους παρόχους υπηρεσιών θεωρώντας ότι τηρούν τη νομοθεσία. Με τα δεδομένα

αυτά, κρίνεται ιδιαίτερα ενδιαφέρουσα η διερεύνηση της γνώσης χρηστών του Διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης (ΜΚΔ) σχετικά με τις ρυθμίσεις που φέρνει ο ΓΚΠΔ στο θέμα της συλλογής και διαχείρισης προσωπικών δεδομένων από οργανισμούς, εταιρείες ή παρόχους και των δικαιωμάτων που οι ίδιοι οι χρήστες έχουν. Συγκεκριμένα, στόχος της παρούσας μεταπτυχιακής διατριβής είναι να μελετήσει αν οι χρήστες, ένα χρόνο σχεδόν μετά την εφαρμογή του νέου Κανονισμού, γνωρίζουν και σε ποιο βαθμό τη νέα νομοθεσία και κατανοούν τις προβλέψεις-δικαιώματα που θεσπίζονται γι' αυτούς. Σε δεύτερο επίπεδο, καθώς η γνώση (δύναται να) επιδρά στη στάση και τη συμπεριφορά, επιχειρείται η ανίχνευση στάσεων και συμπεριφορών των χρηστών στο θέμα της προστασίας της ιδιωτικότητάς τους.

Η παρούσα διπλωματική διατριβή δομείται σε έξι Κεφάλαια. Το πρώτο κεφάλαιο αφορά στις προβλέψεις του ΓΚΠΔ με ειδικότερη αναφορά στα δικαιώματα των υποκειμένων, στις υποχρεώσεις που έχουν οι φορείς, οι οργανισμοί, οι εταιρείες κατά τη διαδικασία επεξεργασίας των δεδομένων, στο ρόλο του υπεύθυνου επεξεργασίας και το θέμα της εκτίμησης του αντικτύπου σχετικά με την προστασία των δεδομένων. Του ΓΚΠΔ έχουν προηγηθεί τόσο ευρωπαϊκές οδηγίες, αλλά και σχετικές εθνικές ρυθμίσεις. Υπό αυτή την έννοια, ο ΓΚΠΔ δεν οικοδομεί κάτι εξ αρχής, αλλά εστιάζει στην ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων και τις διαδικασίες ελέγχου της συμμόρφωσης στη νομοθεσία. Στο πλαίσιο αυτό, το δεύτερο κεφάλαιο αναφέρεται στην ελληνική νομοθεσία για την προστασία των δεδομένων και συγκεκριμένα στον Ν. 2472/97. Το τρίτο κεφάλαιο ασχολείται με το ζήτημα της ιδιωτικότητας στην Κοινωνία της Πληροφορίας, εστιάζοντας σε θέματα όπως οι προκλήσεις που αναδύονται για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, οι ανησυχίες ιδιωτικότητας των χρηστών και οι απόψεις τους για το ρόλο της νομοθεσίας στην προστασία των δεδομένων τους. Το επόμενο κεφάλαιο (τέταρτο) αναφέρεται στο σκοπό της έρευνας, το ερευνητικό πρόβλημα και την οργάνωση της ερευνητικής διαδικασίας. Στο πέμπτο κεφάλαιο παρουσιάζονται τα αποτελέσματα της έρευνας και σχολιάζονται με βάση προηγούμενη βιβλιογραφία και παρελθούσες έρευνες. Τέλος, στο έκτο κεφάλαιο καταγράφονται με συνοπτικό τρόπο τα συμπεράσματα της ερευνητικής διαδικασίας και συζητώνται προτάσεις σε σχέση με τα ερευνητικά ευρήματα. Μετά τις βιβλιογραφικές αναφορές, ακολουθούν τρία Παραρτήματα. Στο πρώτο περιλαμβάνεται πίνακας που παρουσιάζει τη σύγκριση ανάμεσα στις προβλέψεις του ΓΚΠΔ και την προηγουμένως

εφαρμοζόμενη Οδηγία 95/46 ΕΕ. Στο δεύτερο Παράρτημα περιλαμβάνεται το ερευνητικό εργαλείο (ερωτηματολόγιο) και στο τρίτο πίνακες αποτελεσμάτων.

τρίτο πίνακες αποτελεσμάτων.

Κεφάλαιο 1

Ο νέος Ευρωπαϊκός Κανονισμός

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) (Ευρ. Κοινοβούλιο, 679/2016) διαμορφώνει, όπως ήδη αναφέρθηκε, ένα νέο τοπίο αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα εστιάζοντας τόσο σε διαδικασίες συμμόρφωσης των οργανισμών, φορέων ή εταιρειών που συλλέγουν δεδομένα, όσο και στα δικαιώματα των χρηστών.

Πριν γίνει αναλυτική αναφορά στις κυριότερες αλλαγές που επιφέρει ο νέος Κανονισμός¹, κρίνεται σκόπιμη η σύντομη παράθεση ορισμένων βασικών εννοιών, όπως αυτές περιγράφονται αναλυτικά στο άρθρο 4 του Κανονισμού (679/2016 ΕΕ):

➤ **Ανωνυμοποίηση**

Η μεταβολή, αποκοπή, εξάλειψη ή άλλος περιορισμός ή η μετατροπή των Προσωπικών Δεδομένων, ώστε να καταστεί αδύνατη η χρήση τους για αναγνώριση, εντοπισμό ή επικοινωνία με το άτομο.

➤ **Συμβάν Ιδιωτικότητας**

Η παραβίαση ή παράβαση της παρούσας Πολιτικής ή ενός νόμου ιδιωτικότητας ή προστασίας δεδομένων, που περιλαμβάνει ένα Συμβάν Ασφαλείας. Ο καθορισμός του εάν ένα συμβάν ιδιωτικότητας έχει λάβει χώρα και το εάν έχει φυσική υπόσταση διαπιστώνεται από τον Υπάλληλο Προστασίας Δεδομένων και το Νομικό Τμήμα/Τμήμα Συμμόρφωσης.

➤ **Συμβάν Ασφαλείας**

Πρόσβαση από ένα μη εγκεκριμένο πρόσωπο σε Προσωπικά Δεδομένα ή αποκάλυψη σε μη εγκεκριμένο πρόσωπο Προσωπικών Δεδομένων ή η εύλογη υποψία της εταιρείας ότι αυτό συνέβη. Πρόσβαση σε Προσωπικά Δεδομένα από ή για λογαριασμό της εταιρείας χωρίς την πρόθεση να παραβιαστεί η παρούσα

¹ Για τη σύγκριση των προβλέψεων και των αρχών του ΓΚΠΔ σε σχέση με προηγούμενη νομοθεσία (Οδηγία 95/46 ΕΕ) βλ. Παράρτημα Α.

Πολιτική δεν αποτελεί Συμβάν Ασφαλείας, υπό την προϋπόθεση ότι τα συγκεκριμένα Προσωπικά Δεδομένα χρησιμοποιήθηκαν έπειτα και αποκαλύφθηκαν μόνο όπως επιτρέπεται από την παρούσα Πολιτική.

➤ **Ευαίσθητα Δεδομένα**

Οποιοσδήποτε τύπος δεδομένων σχετικά με ανθρώπους που περιέχει εγγενή κίνδυνο πρόκλησης πιθανής βλάβης σε άτομα, συμπεριλαμβανομένων δεδομένων που ορίζονται από το νόμο ως ευαίσθητα, αλλά χωρίς να περιορίζονται σε δεδομένα που σχετίζονται με υγεία, κληρονομικότητα, φυλή, εθνική καταγωγή, θρησκεία, πολιτικές ή φιλοσοφικές πεποιθήσεις ή απόψεις, ποινικό μητρώο, πληροφορίες ακριβούς γεωγραφικής τοποθεσίας, αριθμοί τραπεζικών ή άλλης οικονομικής φύσης λογαριασμών, αριθμοί μητρώου που εκδίδονται από το κράτος, ανήλικα άτομα, σεξουαλική ζωή, σχέσεις με εργατικά συνδικάτα, ασφάλεια, κοινωνική ασφάλεια και άλλες εργοδοτικές ή κρατικές παροχές.

➤ **Τρίτο Πρόσωπο**

Οποιαδήποτε έννομη οντότητα, οργανισμός ή άτομο που δεν ανήκει στην εταιρεία, ή για το οποίο η εταιρεία δεν έχει ελεγκτικό ενδιαφέρον, ή που δεν εργάζεται για την εταιρεία. Εκτός εάν έχει ρητά καθοριστεί από την παρούσα Πολιτική, καμία θυγατρική ή τομέας της εταιρείας δεν απαιτείται να πληροί τις απαιτήσεις ενός τρίτου προσώπου υπό την παρούσα Πολιτική, καθώς όλες οι θυγατρικές και τομείς απαιτείται να επεξεργάζονται δεδομένα σχετικά με ανθρώπους σε συμφωνία με την παρούσα Πολιτική, συμπεριλαμβανομένων των περιπτώσεων όπου μία από τις θυγατρικές της εταιρείας υποστηρίζει μια ή περισσότερες θυγατρικές της εταιρείας κατά την επεξεργασία.

➤ **Επεξεργασία**

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, όπως π.χ. η συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, διάδοση, ανάκτηση, χρήση, διαγραφή, καταστροφή, κ.λπ..

➤ **Υπεύθυνος επεξεργασίας**

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

➤ *Εκτελών την επεξεργασία*

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

1.1 Υποχρεώσεις στη διαδικασία επεξεργασίας Προσωπικών Δεδομένων

Οι βασικές αρχές (άρθρο 5, 679/2016 ΕΕ) που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι :

α) η *νομιμότητα, αντικειμενικότητα και διαφάνεια*, ώστε να διασφαλίζεται ότι τα δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με δίκαιο και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

β) ο *περιορισμός του σκοπού*, ώστε να διασφαλίζεται ότι τα δεδομένα συλλέγονται για συγκεκριμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε άλλη επεξεργασία που είναι ασύμβατη με τους σκοπούς αυτούς. Ασύμβατη δεν κρίνεται η επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς.

γ) η *ελαχιστοποίηση των δεδομένων*, ώστε αυτά να περιορίζονται στα αναγκαία για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

δ) η *ακρίβεια*, ώστε να διασφαλίζεται η ακρίβεια των στοιχείων και αυτά να επικαιροποιούνται, όταν είναι αναγκαίο και σε συμφωνία με την επιθυμητή χρήση τους.

ε) ο *περιορισμός της περιόδου αποθήκευσης*, ώστε τα δεδομένα να διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας τους. Δυνατότητα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα για μεγαλύτερα διαστήματα υπάρχει, εφόσον αυτά υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

στ) η *ακεραιότητα και εμπιστευτικότητα*, ώστε να διασφαλίζεται ότι τα δεδομένα τυγχάνουν επεξεργασίας με τρόπο που εγγυάται την ασφάλεια τους και μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία

απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

ζ) η *λογοδοσία*, ώστε ο υπεύθυνος επεξεργασίας να δύναται να αποδείξει συμμόρφωση με όλα τα παραπάνω.

Στο πλαίσιο των παραπάνω αρχών, ο Κανονισμός επιβάλλει μία σειρά νέων υποχρεώσεων τόσο στους υπεύθυνους επεξεργασίας όσο και στους εκτελούντες την επεξεργασία. Ειδικότερα, αυτές αφορούν:

➤ Λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων.

Λαμβάνοντας υπόψη τις συνθήκες, το κόστος, τα τεχνολογικά μέσα καθώς και τον βαθμό κινδύνου για τις ελευθερίες των υποκειμένων σε περίπτωση παραβίασης, ο υπεύθυνος οφείλει να εφαρμόζει μέτρα για την ασφάλεια των δεδομένων όπως ψευδωνυμοποίηση ή κρυπτογράφηση, διασφάλιση ομαλής λειτουργίας των συστημάτων επεξεργασίας, δυνατότητα αποκατάστασης σε περίπτωση φυσικού ή τεχνικού συμβάντος και τακτικός έλεγχος των μηχανισμών ασφαλείας (Άρθ. 32, 679/2016 ΕΕ).

➤ Προστασία δεδομένων κατά τον σχεδιασμό (Data protection by design)

Ο υπεύθυνος επεξεργασίας έχει υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό των προϊόντων και υπηρεσιών, δημιουργώντας εξ αρχής φιλικές και κατάλληλες συνθήκες για την προστασία των προσωπικών δεδομένων (Άρθ. 25, 679/2016 ΕΕ).

➤ Γνωστοποίηση παραβιάσεων δεδομένων (breach notification):

Αν τα δεδομένα παραβιαστούν και ενδέχεται να προκληθεί παραβίαση των δικαιωμάτων των υποκειμένων, ο υπεύθυνος οφείλει να ενημερώσει την αρμόδια εποπτική αρχή εντός 72 ωρών περιγράφοντας την φύση της παραβίασης, τις συνέπειες που μπορεί να έχει για τα υποκείμενα των δεδομένων και τα ληφθέντα ή προτεινόμενα μέτρα για την αντιμετώπιση του ζητήματος. Σε περίπτωση που ο υπεύθυνος δεν έχει λάβει τα μέτρα που αναφέρονται παραπάνω και η παραβίαση ενδέχεται να θέσει τα υποκείμενα σε υψηλό κίνδυνο, οφείλει, επιπλέον, να ενημερώσει τα ίδια τα υποκείμενα ή να δημοσιοποιήσει πληροφορίες για την παραβίαση (Άρθ. 33 και 34, 679/2016 ΕΕ).

➤ Προστασία δεδομένων εξ ορισμού (data protection by default)

Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα που να διασφαλίζουν εξ ορισμού ότι υφίστανται επεξεργασία

μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας (Άρθ. 25, 679/2016 ΕΕ).

- Ενίσχυση των προϋποθέσεων λήψης της συγκατάθεσης του υποκειμένου
Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης, η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση πρέπει να υποβάλλεται κατά τρόπο, ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (Άρθ. 6, αιτιολογική σκέψη 32, 679/2016 ΕΕ).
- Τήρηση αρχείου των δραστηριοτήτων επεξεργασίας
Κάθε υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία οφείλει να τηρεί –σε γραπτή ή ηλεκτρονική μορφή- αναλυτικό αρχείο των δραστηριοτήτων επεξεργασίας στις οποίες προβαίνει. Σημειώνεται ότι η υποχρέωση τήρησης αρχείου δραστηριοτήτων δεν ισχύει για επιχειρήσεις ή οργανισμούς που απασχολούν λιγότερα από 250 άτομα, εκτός εάν η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η επεξεργασία δεν είναι περιστασιακή ή η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων ή δεδομένα που αφορούν ποινικές καταδίκες (Άρθ. 30, 679/2016 ΕΕ).

1.2. Υπεύθυνος προστασίας δεδομένων (Data Protection Officer)

Μια σημαντική ρύθμιση που επέρχεται με τον ΓΚΠΔ είναι ο ορισμός *υπευθύνου προστασίας δεδομένων* (“Data Protection Officer”). Το πρόσωπο αυτό έχει το ρόλο του θεματοφύλακα των προσωπικών δεδομένων και είναι αρμόδιο, μεταξύ άλλων, (α) να παρακολουθεί τη συμμόρφωση του φορέα με το νόμο, (β) να επικοινωνεί με την αρμόδια εποπτική αρχή και γενικά (γ) να συμβουλεύει τον φορέα για κάθε ζήτημα που άπτεται της προστασίας των δεδομένων προσωπικού χαρακτήρα. Ο υπεύθυνος προστασίας δεδομένων ορίζεται βάσει επαγγελματικών προσόντων και μπορεί να είναι μέλος του προσωπικού του φορέα ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (Άρθ. 37, 679/2016 ΕΕ).

Η υποχρέωση ορισμού υπεύθυνου προστασίας δεδομένων ισχύει σε κάθε περίπτωση, που:

- η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
- οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνίστανται σε πράξεις επεξεργασίας που λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα
- οι βασικές δραστηριότητες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία έχουν να κάνουν με μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (π.χ. δεδομένα που αφορούν την φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, επεξεργασία γενετικών ή βιομετρικών δεδομένων και δεδομένων που αφορούν την υγεία, την σεξουαλική ζωή του φυσικού προσώπου ή τον γενετήσιο προσανατολισμό) και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 του Κανονισμού.

Η επεξεργασία δεδομένων από τον εκτελούντα την επεξεργασία πρέπει να διέπεται υποχρεωτικά από σύμβαση ή άλλη νομική πράξη, η οποία οφείλει να έχει το ειδικό περιεχόμενο που προβλέπει ο Κανονισμός και στην οποία καθορίζονται το αντικείμενο, η διάρκεια, η φύση και ο σκοπός της επεξεργασίας, ο τύπος των δεδομένων προσωπικού χαρακτήρα, οι κατηγορίες των υποκειμένων των δεδομένων και οι υποχρεώσεις, καθήκοντα και δικαιώματα του υπεύθυνου επεξεργασίας (Άρθρο 38, 679/2016 ΕΕ).

1.3 Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (Data Protection Impact Assessment)

Σημαντικό είναι το θέμα της εκτίμησης του αντικτύπου σχετικά με την προστασία δεδομένων (“Data Protection Impact Assessment”). Το Άρθρο 35 του ΓΚΠΔ προβλέπει και προληπτικά μέτρα για την ασφάλεια των υποκειμένων και για την εκτίμηση αντικτύπου. Σύμφωνα με το Άρθρο αυτό, αν η επεξεργασία δεδομένων υπάγεται σε κατηγορία που μπορεί να θέσει σε υψηλό κίνδυνο τα υποκείμενα, ο υπεύθυνος θα πρέπει να συμβουλευτεί τον υπεύθυνο προστασίας δεδομένων πριν προχωρήσει. Οι κατηγορίες υψηλού ρίσκου είναι, μεταξύ άλλων:

- Η συστηματική και εκτενής παρακολούθηση προσωπικών πτυχών των υποκειμένων, όπως η κατάρτιση προφίλ, με σκοπό την λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα για το υποκείμενο
- Η επεξεργασία ειδικής κατηγορίας δεδομένων σε μεγάλη κλίμακα και
- Η συστηματική παρακολούθηση δημοσίων χώρων σε μεγάλη κλίμακα

Ο νέος Κανονισμός ενθαρρύνει, επιπλέον, τη *σύνταξη* κωδίκων δεοντολογίας από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία, οι οποίοι δύνανται να υποβάλλονται προς έγκριση στην αρμόδια εποπτική αρχή. Ομοίως, ενθαρρύνεται και η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων προς απόδειξη της συμμόρφωσης με τον Κανονισμό. Σημειώνεται πως η εκπόνηση κωδίκων δεοντολογίας καθώς και η λήψη πιστοποίησης είναι αμφότερα προαιρετικά (Άρθ. 40-43, 679/2016 ΕΕ).

Κάθε Οργανισμός, λοιπόν, οφείλει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να συμμορφώνεται με τον νέο Κανονισμό. Στα μέτρα αυτά περιλαμβάνονται:

- Η ενσωμάτωση στις διαδικασίες των δικαιωμάτων των υποκειμένων των δεδομένων.
- Η λήψη κατάλληλων μέτρων ασφαλείας και αναγκαίων πολιτικών για την προστασία των πληροφοριών.
- Η εφαρμογή κατάλληλων μέτρων που θα διασφαλίζουν τη διαθεσιμότητα της πληροφορίας (Σχέδιο Επιχειρησιακής Συνέχειας).
- Ο σχεδιασμός προϊόντων και υπηρεσιών λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας (Privacy by Design, Privacy by Default).

- Η σύνταξη σχεδίου αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).
- Η ανάλυση των επιπτώσεων που μπορούν να προκύψουν λόγω παραβίασης της ιδιωτικότητας (Privacy Impact Assessment).
- Ο ορισμός υπεύθυνου για την προστασία των δεδομένων (Data Protection Officer – DPO), όταν συντρέχουν οι προϋποθέσεις.
- Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων όπως ορίζονται από τον ΓΚΠΔ.

Η εφαρμογή των εν λόγω μέτρων αποτελεί πρόκληση για τις επιχειρήσεις και τους οργανισμούς που διαχειρίζονται δεδομένα, αφού σε περίπτωση μη τήρησης του Κανονισμού, προβλέπονται πρόστιμα που φτάνουν τα 20 εκατομμύρια ευρώ. Πρόκληση, όμως, αποτελεί και για τα νομικά συστήματα των κρατών – μελών της Ένωσης που καλούνται να προτείνουν επιμέρους μέτρα, ώστε να διευκολύνουν την εφαρμογή του Κανονισμού στην επικράτεια τους και να διασφαλίσουν την δημιουργία εποπτικής αρχής που θα παρακολουθεί την εφαρμογή των μέτρων και θα φροντίζει για την ομαλή κυκλοφορία των δεδομένων στην Ένωση. Έτσι, αν και ο Γενικός Κανονισμός για την Προστασία των Δεδομένων έρχεται ως ένα αυστηρό νομικό πλαίσιο με σκοπό την δημιουργία ενός ενιαίου πλαισίου διαχείρισης των δεδομένων εντός της Ένωσης, επιτρέπει σε πολλά σημεία εναρμόνιση με το δίκαιο του κάθε κράτους – μέλους.

1.4 Τα δικαιώματα των υποκειμένων των δεδομένων

Πολύ σημαντικό νέο στοιχείο του Κανονισμού είναι οι ρυθμίσεις για τα δικαιώματα των χρηστών. Ο ΓΚΠΔ ενισχύει τα ήδη υφιστάμενα δικαιώματα των υποκειμένων των δεδομένων (π.χ. δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα), ενώ παράλληλα κατοχυρώνει και νέα δικαιώματα.

1. Το δικαίωμα στην Ενημέρωση

Σύμφωνα με το άρθρα 12, 13 και 14 (2016/679 ΕΕ), κατά την συλλογή των δεδομένων, ο διαχειριστής οφείλει να ενημερώσει σε εύλογο χρονικό διάστημα το υποκείμενο των δεδομένων σε σαφή, συνοπτική και εύκολα προσβάσιμη μορφή για την επεξεργασία στην οποία πρόκειται να υποβληθούν τα δεδομένα του και για τα δικαιώματά του. Εξαιρούνται

περιπτώσεις που τα δεδομένα προστατεύονται από απόρρητο ή περιπτώσεις που η απόκτηση και κοινολόγηση τους προβλέπεται από το δίκαιο του κράτους ή της Ένωσης.

Μεταξύ άλλων, ο υπεύθυνος θα πρέπει να παρέχει πληροφορίες για τον ίδιον, τους σκοπούς της επεξεργασίας, τους αποδέκτες των δεδομένων -αν υπάρχουν-, το χρονικό διάστημα που θα διατηρηθούν τα δεδομένα και τα κριτήρια που επηρεάζουν το διάστημα αυτό. Παράλληλα, δηλώνεται με σαφήνεια το δικαίωμα υποβολής αιτήματος (για πρόσβαση, επεξεργασία ή διαγραφή των δεδομένων), το δικαίωμα ανάκλησης της συγκατάθεσης και η δυνατότητα καταγγελίας σε εποπτική αρχή.

Αν τα δεδομένα τυγχάνουν επεξεργασίας με σκοπό την κατάρτιση προφίλ, θα πρέπει να υπάρχει ενημέρωση ξεχωριστά για την διαδικασία και τις συνέπειες που μπορεί να έχει για το υποκείμενο των δεδομένων. Σε περίπτωση που τα δεδομένα διαβιβαστούν σε τρίτους, το υποκείμενο πρέπει να ενημερωθεί το αργότερο μετά την πρώτη διαβίβαση. Το υποκείμενο έχει, επίσης, το δικαίωμα να αιτηθεί ενημέρωση για το κατά πόσο δεδομένα που το αφορούν περνούν από επεξεργασία ή ακόμα και να παραλάβει τα δεδομένα του σε μηχαναγνώσιμη μορφή και να τα διαθέσει σε άλλον υπεύθυνο επεξεργασίας.

Σε περίπτωση που δεδομένα προσωπικού χαρακτήρα υψηλού κινδύνου παραβιαστούν, ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει το υποκείμενο για την φύση της παραβίασης, το είδος των δεδομένων, τις συνέπειες της παραβίασης και τα μέτρα που λαμβάνει για την επίλυση του ζητήματος, ειδικά αν η παραβίαση απειλεί την ασφάλεια ή την καταπάτηση ατομικών δικαιωμάτων των υποκειμένων (Άρθ. 33 και 34, 2016/679 ΕΕ).

2. Το δικαίωμα στην Πρόσβαση, Διόρθωση και Διαγραφή Δεδομένων

Σύμφωνα με τα άρθρα 15, 16 και 17 του Κανονισμού (2016/679 ΕΕ), τα άτομα έχουν το δικαίωμα στην πρόσβαση στα Προσωπικά Δεδομένα τους και στην διόρθωση, τροποποίηση ή διαγραφή αυτών που είναι ανακριβή, ελλιπή ή απαρχαιωμένα. Ο Οργανισμός οφείλει να εγκρίνει όλες τις αιτήσεις για πρόσβαση, διόρθωση και διαγραφή Προσωπικών Δεδομένων, ο δε υπεύθυνος είναι υποχρεωμένος να τις εκτελέσει εφόσον, μεταξύ άλλων:

- Τα δεδομένα δεν είναι πλέον χρήσιμα για τους σκοπούς που συλλέχθηκαν
- Έχει ανακληθεί η συγκατάθεση
- Τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα

Σε περίπτωση που ο υπεύθυνος αρνηθεί να εκτελέσει το αίτημα, το υποκείμενο μπορεί να υποβάλλει αίτημα περιορισμού της επεξεργασίας. Το ίδιο αίτημα μπορεί να κατατεθεί και στην περίπτωση που, ενώ ο υπεύθυνος δεν χρειάζεται πλέον τα δεδομένα, τα χρειάζεται το υποκείμενο για την άσκηση νομικών αξιώσεων (Άρθ. 18, 2016/679 ΕΕ). Εάν μια αίτηση πρόσβασης, διόρθωσης ή διαγραφής ορίζεται από υπάρχουσα Νομοθεσία που παρέχει μεγαλύτερη προστασία για τα άτομα, ο Οργανισμός οφείλει να εξασφαλίζει ότι πληρούνται οι επιπλέον προϋποθέσεις βάσει Νομοθεσίας.

3. *Η Ελεύθερη συγκατάθεση*

Ο ΓΚΠΔ δίνει ιδιαίτερη βαρύτητα στην συγκατάθεση του υποκειμένου για την χρήση προσωπικών δεδομένων, η οποία θα πρέπει να παρέχεται με σαφή θετική ενέργεια που να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου (Άρθ. 7, 2016/679 ΕΕ, αιτιολογική σκέψη 32 ΓΚΠΔ). Η συγκατάθεση θα μπορούσε να δοθεί με μία γραπτή δήλωση, με τη συμπλήρωση τετραγωνιδίου σε μια ιστοσελίδα. Έμφαση δίνεται στην θετική ενέργεια εκ μέρους του υποκειμένου οπότε η σιωπή, τα προ συμπληρωμένα τετραγωνίδια ή η αδράνεια δεν μπορούν να εκλαμβάνονται ως συγκατάθεση (αιτιολογική σκέψη 32 ΓΚΠΔ). Ο Κανονισμός δεν επιτρέπει περιθώρια εξαιρέσεων, αφού η συγκατάθεση θα πρέπει να αφορά συγκεκριμένα δεδομένα που θα υποβληθούν σε ορισμένη επεξεργασία για καθορισμένο χρονικό διάστημα.

Για να διαφυλαχθεί η διαδικασία ορίζεται επιπλέον ότι:

1. Το υποκείμενο μπορεί να αναιρέσει την συγκατάθεσή του οποιαδήποτε στιγμή και ο υπεύθυνος της επεξεργασίας οφείλει να διευκολύνει στην συγκεκριμένη διαδικασία.
2. Η συγκατάθεση δεν θεωρείται ελεύθερη, αν υπάρχουν ξεκάθαρες σχέσεις εξουσίας μεταξύ του υποκειμένου και του υπεύθυνου (π.χ. ο υπεύθυνος της επεξεργασίας είναι δημόσια αρχή). Σε καμία περίπτωση η συγκατάθεση δεν θα πρέπει να είναι προϋπόθεση για την παροχή υπηρεσιών, εκτός αν η χρήση δεδομένων είναι απαραίτητη για την παροχή της υπηρεσίας.

3. Για κάθε άλλη χρήση των δεδομένων, το υποκείμενο θα πρέπει να ενημερώνεται και να δίνει την συγκατάθεση του εκ νέου.

Ειδικότερα όσον αφορά ευαίσθητα δεδομένα, η συγκατάθεση θα πρέπει να δίνεται με ακόμη μεγαλύτερη σαφήνεια. Το άρθρο 9 του Κανονισμού για την «ειδική κατηγορία δεδομένων» απαγορεύει την

επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και [την] επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό (Άρθ. 9, 2016/679 ΕΕ).

Εξαιρέση αποτελούν και πάλι οι περιπτώσεις προστασίας του ατόμου ή των οικείων του, η προστασία του δημόσιου συμφέροντος ή η συλλογή των δεδομένων στα πλαίσια άσκησης της δικαιοσύνης, επιστημονικών ή στατιστικών σκοπών και φυσικά, οι περιπτώσεις που το ίδιο το υποκείμενο έχει δημοσιοποιήσει τα δεδομένα. Τέλος, το άρθρο 8 του Κανονισμού απαγορεύει την χρήση προσωπικών δεδομένων παιδιών κάτω των 16 ετών χωρίς την ελεύθερη συγκατάθεση του γονέα.

4. Το δικαίωμα της Επιλογής

Σε συμφωνία με τις αρχές ιδιωτικότητας για «Σεβασμό» και «Εμπιστοσύνη» και το άρθρο 6 παρ. 1 στοιχ. ε' του Κανονισμού, το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να σταματήσει την εν λόγω επεξεργασία και να εγκρίνει τις ατομικές αιτήσεις ένστασης στην επεξεργασία Προσωπικών Δεδομένων (Άρθ. 21, 2016/679 ΕΕ), συμπεριλαμβανομένης, αλλά χωρίς να περιορίζεται, της επιλογής μη συμμετοχής σε προγράμματα ή δραστηριότητες στις οποίες τα άτομα είχαν προηγουμένως συμφωνήσει να συμμετέχουν, της επεξεργασίας Προσωπικών Δεδομένων τους για σκοπούς απευθείας μάρκετινγκ με στόχο την επικοινωνία που στοχεύει στα υποκείμενα και που βασίζεται σε Προσωπικά Δεδομένα (άρθρο 21 παρ. 2-5, 2016/679 ΕΕ). Το ίδιο ισχύει και για κάθε αξιολόγηση ή λήψη αποφάσεων σχετικά με τα υποκείμενα, η οποία έχει τη δυνατότητα να τα επηρεάσει

σημαντικά και που γίνεται μέσω της χρήσης αλγορίθμων ή αυτοματοποίησης (Άρθ. 22, 2016/679 ΕΕ).

Μόνο εκτός των περιπτώσεων που απαγορεύεται από τη Νομοθεσία (άρθρο 23 παρ. 1 στοιχ. α' - ι', 2016/679 ΕΕ), ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία των δεδομένων μπορεί να αρνηθεί την επιλογή του υποκειμένου να αντιταχθεί στην επεξεργασία δεδομένων που το αφορούν, όταν μια συγκεκριμένη αίτηση δύναται να παρακωλύσει την ικανότητα του Οργανισμού να: (1) συμμορφωθεί με τη Νομοθεσία ή μια ηθική υποχρέωση, συμπεριλαμβανομένης της περίπτωσης να είναι υποχρεωμένος να αποκαλύψει προσωπικά δεδομένα ως απάντηση σε έννομα αιτήματα των δημοσίων αρχών, εξαιτίας προϋποθέσεων των αρχών ασφαλείας ή της εθνικής ασφάλειας, (2) να διερευνήσει, να αμυνθεί ή να ζητήσει νομικές αξιώσεις, και (3) να συνάψει συμβόλαια, να διαχειριστεί σχέσεις, ή να επιτελέσει άλλες επιτρεπόμενες επαγγελματικές δραστηριότητες που συνάδουν με τις αρχές της Διαφάνειας και του Περιορισμού του Σκοπού και που εισήχθησαν βάσει των δεδομένων των ατόμων που σχετίζονται με αυτά.

Ο Οργανισμός οφείλει να απαντά στο άτομο ή στην οντότητα που έθεσε το ερώτημα, παράπονο ή ανησυχία στον Οργανισμό εντός τριάντα (30) ή κατ' ανώτατο όριο εντός εξήντα (60) ημερολογιακών ημερών, εκτός εάν κάποιος Νόμος προβλέπει ή αιτών/ τρίτο πρόσωπο απαιτήσει απάντηση σε μικρότερο χρονικό διάστημα ή εκτός αν οι συνθήκες, όπως μια παράλληλη κρατική έρευνα, απαιτούν μεγαλύτερη χρονική περίοδο. Στην περίπτωση αυτή το άτομο ή ο αιτών/ τρίτο πρόσωπο θα ειδοποιηθεί γραπτώς το συντομότερο δυνατόν που επιτρέπει η γενική φύση των συνθηκών που συνεισφέρουν στην καθυστέρηση.

5. Το δικαίωμα στην μη Κατάρτιση προφίλ

Η κατάρτιση προφίλ είναι μια έννοια που προήλθε από τον χώρο της εγκληματολογίας, ωστόσο, η δυνατότητα συλλογής και επεξεργασίας μεγάλου όγκου δεδομένων την καθιστά συνήθη πρακτική για κάθε είδους Οργανισμό. Ο ΓΚΠΔ, στην προσπάθεια του να ενισχύσει την δυνατότητα των υποκειμένων να προστατεύσουν τα προσωπικά τους δεδομένα, θέτει ορισμένους περιορισμούς στην αυτοματοποιημένη επεξεργασία δεδομένων και την λήψη αποφάσεων χωρίς την εμπλοκή του ανθρώπινου παράγοντα.

Σύμφωνα με το Άρθρο 4 του Κανονισμού, η «κατάρτιση προφίλ» ορίζεται ως

οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

Σε άλλο σημείο του Κανονισμού υπαγορεύεται πως για να οριστεί μια επεξεργασία δεδομένων ως κατάρτιση προφίλ θα πρέπει να υπάρχει η πρόθεση της λήψης αποφάσεων ή η πρόβλεψη των προτιμήσεων, στάσεων ή συμπεριφοράς των φυσικών προσώπων βάσει των αποτελεσμάτων της επεξεργασίας. Παραδείγματα τέτοιων πρακτικών είναι ο σχεδιασμός στοχευμένων εκστρατειών εμπορικής προώθησης.

Ο ΓΚΠΔ προβλέπει μια σειρά από δικαιώματα για τα υποκείμενα των δεδομένων ειδικά ως προς την χρήση προσωπικών δεδομένων με σκοπό την αυτόματη λήψη αποφάσεων, όπως η κατάρτιση προφίλ. Έτσι στα δικαιώματα της ενημέρωσης, της πρόσβασης και της πλήρους συγκατάθεσης πριν την χρήση των προσωπικών δεδομένων (ειδικά αν πρόκειται για ειδική κατηγορία δεδομένων) (άρθρο 6, 2016/679 ΕΕ) προστίθεται το δικαίωμα των υποκειμένων να μην υπόκεινται σε απόφαση με την οποία αξιολογούνται προσωπικές πτυχές που τα αφορούν, λαμβανομένη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο (αιτιολογική σκέψη 71, 2016/679 ΕΕ).

Όσον αφορά την ενημέρωση, το υποκείμενο πρέπει να γνωρίζει τον χρόνο συλλογής δεδομένων με σκοπό την κατάρτιση προφίλ και λεπτομέρειες για την διαδικασία που ακολουθεί ο υπεύθυνος της επεξεργασίας. Ο τελευταίος οφείλει, επιπλέον, να ελέγχει την αξιοπιστία των μέσων που χρησιμοποιεί (τεχνολογία, στατιστικές και μαθηματικές μέθοδοι και οργανωτική δομή), ώστε να αποφεύγονται τα σφάλματα και οι διακρίσεις βάσει των ιδιαίτερων χαρακτηριστικών των υποκειμένων όπως η φυλή, ο σεξουαλικός προσανατολισμός ή η πολιτική πεποίθηση. Σε περίπτωση που για κάποιον λόγο η κατάρτιση προφίλ επιβάλλεται από τον νόμο (π.χ. πάταξη της φοροδιαφυγής ή πρόληψη της απάτης), ή κρίνεται απαραίτητη ή πραγματοποιηθεί μετά την ελεύθερη συγκατάθεση του υποκειμένου,

η επεξεργασία αυτή θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνουν ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, το δικαίωμα διατύπωσης της άποψης του, το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης και το δικαίωμα αμφισβήτησης της απόφασης (αιτιολογική σκέψη 71, 2016/679 ΕΕ).

Να σημειωθεί πως ο Κανονισμός υπογραμμίζει ότι οι παραπάνω περιορισμοί αφορούν μόνο σε αποφάσεις λαμβανόμενες αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας. Ως παραδείγματα παραθέτει τις περιπτώσεις άρνησης αιτήματος επιγραμμικής πίστωσης ή τις ηλεκτρονικές προσλήψεις χωρίς ανθρώπινη παρέμβαση.

Ακόμα και αν η κατάρτιση προφίλ είναι καθ' όλα νόμιμη, το υποκείμενο έχει δικαίωμα να αντιταχθεί οποιαδήποτε στιγμή στην επεξεργασία και ο υπεύθυνος υποχρεούται να παύσει την επεξεργασία δεδομένων, εκτός αν καταδείξει επιτακτικούς και νόμιμους λόγους για αυτήν, οι οποίοι υπερσχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (Άρθ. 21, 2016/679 ΕΕ). Από την άλλη, αν τα δεδομένα υπόκεινται σε επεξεργασία για σκοπούς εμπορικής προώθησης και το υποκείμενο αντιταχθεί, ο υπεύθυνος δεν μπορεί να επικαλεστεί κάποιον λόγο για την συνέχισή της και τα δεδομένα αυτά δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς (άρθρο 21 παρ. 3, 2016/679 ΕΕ).

Ένας από τους σοβαρούς κινδύνους της κατάρτισης προφίλ και της αυτοματοποιημένης λήψης αποφάσεων είναι ότι ενδέχεται να πραγματοποιούνται χωρίς διαφάνεια. Τα υποκείμενα των δεδομένων μπορεί να μην γνωρίζουν ότι τα στοιχεία που παρέχουν οδηγούν στην κατάρτιση προφίλ σχετικά με αυτά, ή να μην κατανοούν πλήρως τι συνεπάγεται αυτό. Παράλληλα, η κατάρτιση προφίλ μπορεί να συμβάλει στη διαίωνιση των υπάρχοντων στερεότυπων και τον κοινωνικό διαχωρισμό. Μπορεί, επίσης, να οριοθετήσει/εντάξει ένα άτομο σε μία συγκεκριμένη κατηγορία και να το περιορίσει σε συγκεκριμένες προτεινόμενες προτιμήσεις. Αυτό μπορεί να υπονομεύσει την ελευθερία της επιλογής, για παράδειγμα μεταξύ προϊόντων ή υπηρεσιών, όπως βιβλία, μουσική ή ενημέρωσή. Σε ορισμένες περιπτώσεις ενδέχεται, επίσης, να οδηγήσει σε ανακριβείς προβλέψεις, άρνηση παροχής υπηρεσιών και αγαθών και αδικαιολόγητες διακρίσεις.

1.5. Εποπτική Αρχή

Το άρθρο 51 του Κανονισμού προβλέπει ότι κάθε κράτος-μέλος φροντίζει, ώστε μία ή περισσότερες ανεξάρτητες δημόσιες αρχές που αποκαλούνται «εποπτική αρχή» θα αναλάβουν την παρακολούθηση της εφαρμογής του Κανονισμού, ενώ προβλέπει παράλληλα και την συνεργασία των εποπτικών αρχών για τη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την Ένωση.

Η ρυθμιστική αρχή στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) που ιδρύθηκε με τον Ν. 2472/1997 και λειτουργεί ως μια συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή. Η διενέργεια διοικητικών ελέγχων καθώς και η εξέταση σχετικών καταγγελιών, προσφυγών και ερωτημάτων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων, όταν αυτά θίγονται από την επεξεργασία δεδομένων, περιλαμβάνονται μεταξύ των ελεγκτικών αρμοδιοτήτων της Αρχής. Η Α.Π.Δ.Π.Χ έχει το δικαίωμα να ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διεξάγοντας διοικητικούς ελέγχους σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Οι έλεγχοι διενεργούνται από υπαλλήλους του Τμήματος των Ελεγκτών, οι οποίοι συνοδεύονται σε ορισμένες περιπτώσεις από μέλη της Αρχής.

Σημειώνεται πως οι ειδικοί ανακριτικοί υπάλληλοι έχουν δικαίωμα πρόσβασης σε κάθε αρχείο, χωρίς να μπορεί να τους αντιταχθεί κανενός είδους απόρρητο. Κατόπιν διενέργειας των απαιτούμενων ελέγχων, η Αρχή μπορεί να επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους διοικητικές κυρώσεις για παράβαση των υποχρεώσεών τους ή για οποιαδήποτε άλλη παράβαση πλήττει τα δικαιώματα των χρηστών όσον αφορά την προστασία των προσωπικών τους δεδομένων. Τέλος, η Αρχή δύναται να καταγγέλλει τις παραβάσεις των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

Κεφάλαιο 2

Η Ελληνική Νομοθεσία

Ο νέος Κανονισμός Προστασίας Προσωπικών Δεδομένων (2016/679 ΕΕ) αν και δεν παρεκκλίνει ουσιωδώς από τις γενικές αρχές του υφιστάμενου ελληνικού πλαισίου προστασίας των προσωπικών δεδομένων (Νόμος 2472/97), δημιουργεί, ωστόσο, ένα αυστηρότερο θεσμικό πλαίσιο επεξεργασίας των προσωπικών δεδομένων και κατ' επέκταση προστασίας τους. Ο ΓΚΠΔ χαρακτηρίζεται από την ριζική αλλαγή του συστήματος ευθύνης για την τήρηση της νομοθεσίας εισάγοντας την αρχή της Λογοδοσίας (Accountability Principle), σύμφωνα με την οποία οι εταιρείες που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα οφείλουν να διαμορφώσουν τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματα τους κατά τέτοιο τρόπο ώστε να είναι πλήρως συμμορφωμένες με όσα προβλέπει ο Κανονισμός. Το βάρος απόδειξης μεταφέρεται από τις Αρχές Προστασίας Προσωπικών Δεδομένων στις εταιρείες, οι οποίες οφείλουν να αποδεικνύουν σε οποιαδήποτε περίπτωση ελέγχου ότι είναι πλήρως εναρμονισμένες με τις διατάξεις του Κανονισμού.

Όσον αφορά την ελληνική νομοθεσία, ο Νόμος 2472/97 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» έχει τροποποιηθεί, ώστε να συνάδει με τις εξελίξεις της Κοινωνίας της Πληροφορίας, προκειμένου να διασφαλίζεται και νομικά η διαφύλαξη των προσωπικών δεδομένων και του ιδιωτικού βίου. Οι τροποποιήσεις που έχουν ενσωματωθεί στον Νόμο 2472/1997 είναι οι εξής:

- **Κανονιστική Πράξη 1/1999** - Ενημέρωση υποκειμένου των δεδομένων κατ' άρθρο 11 Ν.2472/1997
- **Νόμος 3917/2011**. Αφορά τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

- **Οδηγία (ΕΕ) 2016/680** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- **Απόφαση με αριθμό 26/2004**, όπου καθορίζονται οι όροι για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.
- **Απόφαση 408 (11 Δεκεμβρίου 1998)**. Αφορά την ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου.
- **Νόμος 3783/2009**. Σκοπός του νόμου αυτού είναι η ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας προπληρωμένου χρόνου ομιλίας, συνδρομητών με συμβόλαιο, ή άλλης μορφής κινητής τηλεπικοινωνίας, για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.
- **Νόμος 3471/2006**. Σκοπός των διατάξεων των άρθρων 1 έως 17 του νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.
- **ΦΕΚ Β' 3433/31.12.2013**. Κοινή Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) ως προς τις υποχρεώσεις των παροχών για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του ν. 3917/2011, όπως ισχύει («Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»).

2.1. Ο Νόμος 2472/97

Στόχος του νόμου 2472/1997, που ακολουθεί την Οδηγία 95/46/EK, είναι η θέσπιση προϋποθέσεων στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με λίγα λόγια, ο νόμος 2472/1997 καθορίζει τις υποχρεώσεις των φορέων και των υπηρεσιών που «εκτελούν την επεξεργασία» και θέτει τα δικαιώματα προστασίας των ατόμων, όσον αφορά στην προστασία και διαφύλαξη των προσωπικών τους δεδομένων.

Στο άρθρο 2 του ν. 2472/1997 καθορίζονται ως δεδομένα προσωπικού χαρακτήρα κάθε πληροφορία που αναφέρεται σε συγκεκριμένο φυσικό πρόσωπο που προσδιορίζεται ή μπορεί να προσδιορισθεί. Το φυσικό αυτό πρόσωπο είναι το υποκείμενο των δεδομένων προσωπικού χαρακτήρα. Δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα τα στατιστικά στοιχεία και αυτά που αφορούν σε νομικά πρόσωπα.

Τα προσωπικά δεδομένα διακρίνονται σε δύο κατηγορίες. Τα «*Ευαίσθητα*», η επεξεργασία των οποίων κατ' αρχήν δεν επιτρέπεται. Αυτά περιλαμβάνουν δεδομένα που αφορούν την φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία και κοινωνική πρόνοια, την ερωτική ζωή, ποινικές διώξεις ή καταδίκες και συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Η δεύτερη κατηγορία περιλαμβάνει τα «*Κοινά*» προσωπικά δεδομένα, η επεξεργασία των οποίων κατ' αρχήν επιτρέπεται. Στην κατηγορία αυτή ανήκουν όσα δεν εντάσσονται στην πρώτη.

Το άρθρο 5 του ν. 2472/1997 αναφέρεται στη συγκατάθεση του υποκειμένου, τη δήλωση δηλαδή της βούλησής του ότι δέχεται τα δεδομένα που το αφορούν να γίνουν αντικείμενο επεξεργασίας. Η συγκατάθεση είναι ελεύθερα ανακλητή χωρίς αναδρομικό αποτέλεσμα. Η δήλωση βούλησης πρέπει να είναι ελεύθερη, συνειδητή, ρητή, σαφώς εκφρασμένη και ειδική. Δεν απαιτείται συγκατάθεση, όταν η επεξεργασία είναι αναγκαία:

- για την εκτέλεση σύμβασης στην οποία το υποκείμενο συμβάλλεται
- για ενέργειες κατά το προσυμβατικό στάδιο μετά από αίτηση του υποκειμένου.
- για την εκπλήρωση υποχρέωσης του υποκειμένου που επιβάλλεται από νόμο.

- για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να συγκατατεθεί.
- για λόγους δημοσίου συμφέροντος ή αν εμπίπτει στην άσκηση δημόσιας εξουσίας.
- για την ικανοποίηση του εννόμου συμφέροντος του υπεύθυνου επεξεργασίας ή των αποδεκτών των δεδομένων, υπό τον όρο ότι το έννομο συμφέρον αυτό υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των υποκειμένων των δεδομένων.

Το άρθρο 6 του ν. 2472/1997 αφορά στην γνωστοποίηση. Κάθε αρχείο που λειτουργεί ή πρόκειται να λειτουργήσει πρέπει να γνωστοποιείται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα από τον υπεύθυνο επεξεργασίας. Η γνωστοποίηση πρέπει κατ'ελάχιστο να περιλαμβάνει:

- την ταυτότητα του υπεύθυνου επεξεργασίας.
- τη διεύθυνση εγκατάστασης του αρχείου.
- τον σκοπό της επεξεργασίας.
- το είδος των δεδομένων.
- το χρόνο τήρησης των δεδομένων.
- τους αποδέκτες των δεδομένων.
- τα βασικά χαρακτηριστικά του συστήματος που χρησιμοποιείται και των μέτρων ασφαλείας του αρχείου (με έμφαση στην εξασφάλιση του απορρήτου της επεξεργασίας).

Από την υποχρέωση γνωστοποίησης εξαιρούνται οι επεξεργασίες δεδομένων που αφορούν:

- σε σχέση εργασίας ή έργου ή παροχής υπηρεσιών
- σε πελάτες ή προμηθευτές και δεν διαβιβάζονται σε τρίτους εκτός εάν πρόκειται για:
 - ασφαλιστικές εταιρίες
 - εταιρείες εμπορίας πληροφοριών
 - τράπεζες
 - εταιρείες έκδοσης πιστωτικών καρτών
- σε μέλη ή εταίρους σωματείων, εταιριών ή ενώσεων προσώπων και δεν διαβιβάζονται σε τρίτους

- σε δεδομένα υγείας από ιατρούς ή άλλους παρόχους υπηρεσιών υγείας, τα οποία δεν διαβιβάζονται σε τρίτους και ο υπεύθυνος επεξεργασίας υποχρεούται να τηρεί το απόρρητο αυτών
- στην άσκηση επαγγέλματος από συμβολαιογράφους, δικηγόρους, δικαστικούς επιμελητές κ.λπ. εφόσον τα δεδομένα δεν διαβιβάζονται σε τρίτους και ο υπεύθυνος επεξεργασίας υποχρεούται να τηρεί το απόρρητο αυτών
- στην απονομή της δικαιοσύνης ή για την εξυπηρέτηση αναγκών λειτουργίας δικαστικών αρχών ή υπηρεσιών στο πλαίσιο απονομής δικαιοσύνης

Για τα ευαίσθητα δεδομένα, σύμφωνα με το άρθρο 7 του Ν. 2472/97, η επεξεργασία επιτρέπεται κατ' εξαίρεση μόνο μετά από άδεια της Αρχής. Η άδεια χορηγείται μόνο υπό συγκεκριμένες περιοριστικά αναφερόμενες προϋποθέσεις, ισχύει για ορισμένο χρόνο και μπορεί να ανανεωθεί μετά από νέα αίτηση.

Ο υπεύθυνος επεξεργασίας των δεδομένων οφείλει να λαμβάνει τα κατάλληλα οργανωτικά μέτρα για τη διασφάλιση του απορρήτου, να καταστρέφει τα δεδομένα μετά το πέρας της επεξεργασίας και να εφαρμόζει συγκεκριμένη διαδικασία καταστροφής των δεδομένων (οδηγία 1/2005 Αρχής, άρθ. 10, Ν. 2472/1997).

Για τη διασύνδεση των αρχείων, τη δυνατότητα δηλαδή συσχέτισης των δεδομένων ενός αρχείου με τα δεδομένα άλλου αρχείου, σύμφωνα με το άρθρο 8 του ν. 2472/1997 είναι απαραίτητη η γνωστοποίηση στην Αρχή και απαιτείται άδεια αυτής εάν αφορά σε ευαίσθητα δεδομένα και εάν χρησιμοποιείται ενιαίος κωδικός αριθμός.

Το άρθρο 16 του ν. 2472/1997 αναφέρεται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μια Ανεξάρτητη Διοικητική Αρχή που προβλέπεται στο Σύνταγμα (άρθρο 9Α) και υπάγεται στο Υπ. Δικαιοσύνης. Ο σκοπός της είναι να εκδίδει οδηγίες και κανονιστικές πράξεις για την εφαρμογή του νόμου, να ενεργεί ελέγχους σε αρχεία αυτεπάγγελτα ή μετά από καταγγελία, να επιβάλλει διοικητικές κυρώσεις για παράβαση του νόμου και να χορηγεί τις άδειες που προβλέπονται στο νόμο. Συνεργάζεται με τις αντίστοιχες Αρχές των άλλων κρατών – μελών και οι εκπρόσωποι των Αρχών των κρατών – μελών, συγκροτούν την Ομάδα του άρθρου 29 της Οδηγίας 95/46/ΕΚ που λειτουργεί ως συμβουλευτικό και γνωμοδοτικό όργανο της Επιτροπής της Ε.Ε.

2.2. Τα δικαιώματα των υποκειμένων

Κάθε υποκείμενο δεδομένων έχει, σύμφωνα με τον Ν. 2472/92:

- *Δικαίωμα ενημέρωσης (Άρθρο 11 Ν. 2472/1997)*

Κάθε υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει το υποκείμενο κατά την έναρξη της επεξεργασίας – στο στάδιο της συλλογής των δεδομένων – για τα εξής τουλάχιστον στοιχεία: Την ταυτότητα του υπεύθυνου επεξεργασίας, τον σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων, καθώς και την ύπαρξη δικαιώματος πρόσβασης. Η ενημέρωση πρέπει να γίνεται κατά τρόπο σαφή και πρόσφορο. Εφόσον τα δεδομένα ενός αρχείου αφορούν μεγάλο αριθμό υποκειμένων (άνω των 1.000), η ενημέρωσή τους μπορεί να γίνει και δια του τύπου με απόφαση της Αρχής. Η υποχρέωση ενημέρωσης μπορεί να αρθεί με απόφαση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

- *Δικαίωμα πρόσβασης (Άρθρο 12 Ν. 2472/1997)*

Κάθε υποκείμενο έχει δικαίωμα να ζητά και να λαμβάνει από τον υπεύθυνο επεξεργασίας τις ακόλουθες πληροφορίες: όλα τα υπό επεξεργασία δεδομένα που το αφορούν, την προέλευσή τους, τον σκοπό της επεξεργασίας, τους αποδέκτες, τη λογική της αυτοματοποιημένης επεξεργασίας, την τυχόν διόρθωση, διαγραφή ή δέσμευση των δεδομένων που το αφορούν καθώς και στην κοινοποίηση σε τρίτους. Η σχετική αίτηση πρέπει να απαντηθεί εντός 15 ημερών, ενώ το δικαίωμα πρόσβασης μπορεί να αρθεί μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

- *Δικαίωμα αντίρρησης (Άρθρο 13 Ν. 2472/1997)*

Κάθε υποκείμενο έχει δικαίωμα να υποβάλει αντιρρήσεις στον υπεύθυνο επεξεργασίας για την επεξεργασία των δεδομένων που το αφορούν. Στο πλαίσιο αυτό, απαιτείται έγγραφο με συγκεκριμένο αίτημα για ενέργεια όπως διόρθωση, μη χρησιμοποίηση, μη διαβίβαση ή διαγραφή. Στο υποκείμενο των δεδομένων οφείλεται έγγραφη απάντηση εντός δεκαπέντε (15) ημερών, στην οποία αναφέρονται οι ενέργειες για την ικανοποίηση της αίτησης ή οι λόγοι απόρριψής της. Εάν η αίτηση ικανοποιηθεί, επιστρέφεται το χρηματικό ποσό που κατέβαλε το υποκείμενο κατά την άσκηση του δικαιώματος πρόσβασης. Εάν η αίτηση απορριφθεί, η απάντηση κοινοποιείται στην Αρχή.

Υποσύνολο του δικαιώματος αντίρρησης είναι το δικαίωμα κάθε υποκειμένου να δηλώσει στην Αρχή ότι δεν επιθυμεί την επεξεργασία των δεδομένων του για λόγους marketing ή παροχής υπηρεσιών από απόσταση. Η Αρχή τηρεί ειδικό αρχείο με τα στοιχεία αυτών των υποκειμένων και κάθε υπεύθυνος επεξεργασίας υποχρεούται να το συμβουλευτεί και να απέχει από επεξεργασία τέτοιου σκοπού.

- *Δικαίωμα προσωρινής δικαστικής προστασίας (Άρθρο 14 Ν. 2472/1997)*

Αφορά αποκλειστικά την αυτοματοποιημένη επεξεργασία δεδομένων που έχει σκοπό την αξιολόγηση της προσωπικότητας ή / και της συμπεριφοράς του υποκειμένου, την αποδοτικότητα στην εργασία, την φερεγγυότητα και την αξιοπιστία. Το αίτημα αφορά στην αναστολή ή μη εφαρμογή πράξης ή απόφασης που είναι αποτέλεσμα αυτής της επεξεργασίας και απευθύνεται στο κατά περίπτωση αρμόδιο Δικαστήριο, ακόμη και αν δεν συντρέχουν οι λοιπές προϋποθέσεις δικαστικής προστασίας.

Κεφάλαιο 3

Η Ιδιωτικότητα στην Κοινωνία της Πληροφορίας

Με την ανάδυση της Κοινωνίας της Πληροφορίας, καταδεικνύεται εμφατικά ο ρόλος που έχουν οι νέες τεχνολογίες στην καθημερινότητα και η αξία της πληροφορίας, ενώ ταυτόχρονα εγείρονται κίνδυνοι που αφορούν στα ατομικά δικαιώματα και την ασφάλεια των προσωπικών δεδομένων (Σιδερή, Κίτσιου, Τζωρτζάκη, Καλλονιάτης & Γκρίτζαλης 2017). Οι κίνδυνοι αυτοί προκύπτουν γιατί κοινωνικές, οικονομικές και πολιτικές λειτουργίες των κρατών εξαρτώνται άμεσα από τις πληροφορίες που διακινούνται στα πληροφοριακά συστήματα, τα οποία όμως εξαρτώνται και από τον ιδιωτικό τομέα (Κάλλας 2006, Cebrian 2000). Έτσι ανθρώπινες ενέργειες και αποφάσεις που «σχετίζονται με τον έλεγχο και τη χρήση της πληροφορίας ανάλογα με τα έκδηλα και λανθάνοντα συμφέροντα των κοινωνικών ομάδων που εξυπηρετούν» (Σιδερή κ.α. 2017: 139) επιδρούν θετικά στην ανάπτυξη αυτών των κινδύνων.

Το ζήτημα της ιδιωτικότητας (privacy) και της προστασίας της δεν είναι ένα νέο θέμα. Η κατοχύρωση των ατομικών δικαιωμάτων το 18ο και 19ο αιώνα επέτρεψε τη διατύπωση του δικαιώματος στην ιδιωτικότητα ως άμεσα συνδεδεμένο με την προσωπική ελευθερία, οδηγώντας τελικά στη θέσπιση της νομικής προστασίας της (Σιδερή κ.α. 2017). Το δικαίωμα σεβασμού της ιδιωτικής ζωής αναγνωρίστηκε ως ένα από τα θεμελιώδη προστατευόμενα ανθρώπινα στην Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου το 1948, ενώ μερικά χρόνια αργότερα επιβεβαιώθηκε και σε επίπεδο Ευρώπης με την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (European Union Agency for Fundamental Rights 2018). Ωστόσο η ιδιωτικότητα και η προστασία της τέθηκαν ξανά ως θέμα συζήτησης στο πλαίσιο της εγκαθίδρυσης της Κοινωνίας της Πληροφορίας. Και τούτο, γιατί μετά την τεχνολογική εξέλιξη, η κλασική αντίληψη της ιδιωτικότητας έχει εμπλουτιστεί (Μήτρου 2010: 508-509), ενώ, επιπλέον, καθώς οι σχέσεις μεταξύ των φορέων που διαχειρίζονται την πληροφορία έγιναν αρκετά

πολύπλοκες, η διάκριση μεταξύ ιδιωτικού και δημόσιου κατέστη ακόμα πιο δυσδιάκριτη (Marx 2001).

Σειρά περιστατικών που έρχονται στο φως της δημοσιότητας αποκαλύπτουν μη εξουσιοδοτημένη χρήση των προσωπικών δεδομένων των ατόμων που συνεπάγεται προσβολή της ιδιωτικότητας και των ατομικών τους δικαιωμάτων. Κυβερνήσεις και επίσημοι φορείς χρησιμοποιούν τεχνικές πληθοπορισμού για να ανιχνεύσουν αντιλήψεις και στάσεις των πολιτών, την ώρα που οργανώνουν προγράμματα μαζικής παρακολούθησης αυτών στο όνομα της εθνικής ασφάλειας. Ταυτόχρονα, εταιρείες συγκροτούν το προφίλ των πελατών τους με στόχο την προώθηση και πώληση προϊόντων και εταιρείες παροχής υπηρεσιών,, όπως το Facebook, παρέχουν πρόσβαση στα δεδομένα των χρηστών τους σε τρίτους. Έτσι, δισεκατομμύρια προσωπικά δεδομένα συλλέγονται, παρά την συνταγματική κατοχύρωση του δικαιώματος της ιδιωτικότητας, εν αγνοία συχνά των υποκειμένων των δεδομένων.

3.1 Προκλήσεις στην προστασία της ιδιωτικότητας

Το δικαίωμα στην ιδιωτικότητα και το δικαίωμα στην προστασία των προσωπικών δεδομένων συνδέονται στενά, καθώς προστατεύουν παρόμοιες ανθρώπινες αξίες, όπως την αυτονομία του ατόμου και την ανθρώπινη αξιοπρέπεια, διασφαλίζοντας την ύπαρξη μιας ιδιωτικής σφαίρας ζωής όπου τα άτομα μπορούν να αναπτύξουν ελεύθερα την προσωπικότητά τους και να εκφραστούν. Υπό την έννοια αυτή αποτελούν προϋπόθεση για την άσκηση άλλων θεμελιωδών ελευθεριών. Ωστόσο τα δύο δικαιώματα διαφοροποιούνται μεταξύ τους ως προς τη διατύπωση και το πεδίο εφαρμογής τους (European Union Agency for Fundamental Rights 2018). Το δικαίωμα στην ιδιωτικότητα έχει προσδιοριστεί ως «το δικαίωμα των πολιτών σε μία ανενόχλητη προσωπική ζωή» (Warren & Brandeis 1890) και συνίσταται σε γενική απαγόρευση παρεμβάσεων στην ιδιωτική ζωή, ενώ η προστασία των προσωπικών δεδομένων είναι ένα σύγχρονο ατομικό δικαίωμα που θεμελιώνεται στην ανάγκη προστασίας των ατόμων όταν τα προσωπικά τους δεδομένα επεξεργάζονται (European Union Agency for Fundamental Rights 2018).

Οι νέες τεχνολογίες του διαδικτύου και των εφαρμογών που βασίζονται σε αυτό, όπως τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ), γεννούν σημαντικές νέες προκλήσεις για την προστασία του δικαιώματος στην ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων. Κι αυτό γιατί οι τεχνολογικές εξελίξεις έχουν οδηγήσει σε εργαλεία συλλογής προσωπικών πληροφοριών, με όγκο και μορφή που στο παρελθόν θα ήταν δύσκολο να συγκεντρωθεί και να αναλυθεί. Δημιουργούνται, έτσι, νέες δυνατότητες για κυβερνητικούς και ιδιωτικούς φορείς στην αποθήκευση και επεξεργασία προσωπικών δεδομένων με εξειδικευμένες τεχνικές που επιτρέπουν την ανάλυσή τους, ενώ αύξηση του κινδύνου για τα προσωπικά δεδομένα προκαλεί και η δυνατότητα εντοπισμού κάθε συσκευής μέσα από την οποία αυτά διαχέονται. Παράλληλα, ο όγκος αυτός των δεδομένων που ρέει μέσα στις ψηφιακές πλατφόρμες γεννά νέες ευκαιρίες για την με κάθε τρόπο εμπορική χρήση τους.

Έτσι αναδύεται μια σειρά απειλών για τα υποκείμενα των δεδομένων αναφορικά με τον έλεγχο των προσωπικών τους δεδομένων και τη διαφύλαξη της ιδιωτικότητάς τους. Στους κινδύνους αυτούς συμβάλει ο ρόλος και η ευθύνη των παρόχων υπηρεσιών και τρίτων, οι ιδιαίτερες προκλήσεις που δημιουργούν οι διάφορες εφαρμογές, οι πλατφόρμες επικοινωνίας και τα επιχειρηματικά μοντέλα, συμπεριλαμβανομένου του cloud computing, των μηχανών αναζήτησης, των ψηφιακών κοινωνικών δικτύων και των φορητών συσκευών, τα προβλήματα που αναδύονται με την αξιοποίηση μοντέλων πληθοπορισμού, αλλά και οι απειλές που δημιουργούνται από διάφορους μηχανισμούς επιτήρησης και συλλογής δεδομένων, όπως τα cookies, κακόβουλα λογισμικά και εργαλεία αναγνώρισης προσώπου και επιτήρησης.

Ως απάντηση σε αυτούς τους κινδύνους, προέκυψε μια σειρά νομικών κειμένων για την προστασία των δεδομένων από τη δεκαετία του 1980, ενώ το 1981 το Συμβούλιο της Ευρώπης προχώρησε στη σύμβαση για την προστασία των ατόμων αναφορικά με την αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων (Σύμβαση 108)(Bhaimia 2018). Παρά το γεγονός, όμως, ότι η νομοθεσία έχει καθορίσει τις γενικές αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα, τα κράτη έχουν διαφορετική αφετηρία νομικού πολιτισμού (Μήτρου 2002) με αποτέλεσμα να χρησιμοποιούν διαφορετικούς ορισμούς των προσωπικών δεδομένων και να εφαρμόζουν διαφορετικούς κανόνες που διέπουν τη συλλογή και χρήση τους.

Το κανονιστικό πλαίσιο της προστασίας της ιδιωτικότητας αφορά στην εφαρμογή διεθνών συμβάσεων δικαίου, εξειδικευμένης εθνικής νομοθεσίας, αποφάσεων ανεξάρτητων αρχών που διαχειρίζονται ζητήματα της Κοινωνίας της Πληροφορίας, αλλά και κανόνων φορέων ιδιωτικού τομέα. Τα πρότυπα προστασίας της ιδιωτικότητας βασίζονται σε μεγάλο βαθμό στις οκτώ αρχές προστασίας της ιδιωτικότητας του ΟΟΣΑ : 1. Περιορισμός συλλογής, 2. Ποιότητα δεδομένων, 3. Προδιαγραφή του σκοπού, 4. Περιορισμός χρήσης, 5. Ασφάλεια, 6. Διαφάνεια 7. Ατομική συμμετοχή, και 8. Λογοδοσία (Hughes 2015).

Τόσο η νομοθεσία όσο και η δημόσια πολιτική αντιμετωπίζουν σημαντικές δυσκολίες να ακολουθήσουν τα νέα δεδομένα που προκύπτουν από την ταχύτατη τεχνολογική ανάπτυξη του διαδικτύου και των εφαρμογών του. Έτσι και παρά τη δήλωση της Ευρωπαϊκής Ένωσης ότι καθένας έχει το δικαίωμα στην προστασία των προσωπικών δεδομένων που τον αφορούν, τίθεται ο προβληματισμός αν πράγματι τα υποκείμενα των δεδομένων γνωρίζουν ότι τα δεδομένα τους συλλέγονται και αν κατανοούν τον τρόπο με τον οποίο συγκεντρώνονται, διατηρούνται, μεταποιούνται, χρησιμοποιούνται και αποκαλύπτονται. Στο πλαίσιο αυτό, ερευνητική μελέτη της Ευρωπαϊκής Επιτροπής το 2011 κατέγραψε τις ανησυχίες των χρηστών σχετικά με την προστασία των δεδομένων τους σε ιστοτόπους κοινωνικής δικτύωσης, ενώ περιέλαβε, επίσης, στοιχεία για αναγκαίες μεταρρυθμίσεις στην Οδηγία 95/46 / ΕΚ για την προστασία των προσωπικών δεδομένων.

3.2 Οι ανησυχίες ιδιωτικότητας των χρηστών

Ο Westin ορίζει ως ιδιωτικότητα το δικαίωμα να αυτό-καθορίζουν τα άτομα ποιες πληροφορίες είναι προσβάσιμες, σε ποιον και πότε, ενώ ο Altman αναφέρεται στην ιδιωτικότητα ως τον επιλεκτικό έλεγχο των ατόμων για την πρόσβαση άλλων στον εαυτό τους, κάνοντας λόγο ουσιαστικά για μια διαδικασία καθορισμού ορίων στο πλαίσιο κοινωνικών αλληλεπιδράσεων (Ziegele & Quiring 2011, Taddicken 2014).

Αν και οι χρήστες συχνά πιστεύουν ότι μπορούν να ελέγξουν την πληροφορία που κοινοποιούν, ελέγχοντας έτσι και την ιδιωτικότητα, οι Conger, Pratt & Loch (2013) επισημαίνουν ότι η πληροφορία σήμερα δεν βρίσκεται υπό των έλεγχο των ατόμων, αλλά

των οργανισμών που κατέχουν την πληροφορία. Αυτό εξηγεί και μια σειρά από συμβάντα που τα υποκείμενα των πληροφοριών βιώνουν ή πληροφορούνται. Συμβάντα που κυμαίνονται από την διαρροή των προσωπικών δεδομένων ως τις γνωστές στο διαδίκτυο στοχευμένες διαφημίσεις και τα οποία επιτείνουν τις ανησυχίες ιδιωτικότητας των χρηστών του Διαδικτύου και των ΜΚΔ, καθώς αναγνωρίζουν ότι κάποιιοι εισβάλλουν τελικά με πολλούς τρόπους και μέσω πολλών οδών στην προσωπική τους ζωή. Μάλιστα, οι αγωνίες αυτές θα μεγεθύνονται ακόμη περισσότερο, καθώς η χρήση των κινητών συσκευών βαίνει αυξανόμενη (Benson, Saridakis & Tennakoon 2015).

Παρά το γεγονός ότι τα υποκείμενα των δεδομένων εκφράζουν ανησυχίες για την προστασία τους, τα ίδια αποκαλύπτουν δεδομένα τους, εκούσια ή ακούσια, συνειδητά ή μη συνειδητά. Αποτυγχάνουν, όπως εξηγεί ο Baek (2014), τελικά να μεταφράσουν τις ανησυχίες τους για την ιδιωτικότητα στα ψηφιακά περιβάλλοντα σε συμπεριφορές προστασίας της ιδιωτικότητας (privacy protective behavior). Η Taddicken (2014) επισημαίνει ότι η ιδεατή επίτευξη της ψηφιακής ιδιωτικότητας συνίσταται σε μια ισορροπημένη σχέση μεταξύ της ανάγκης για κοινωνική αλληλεπίδραση και αυτής της προστασίας της ιδιωτικότητας.

Πολλές προτάσεις έχουν διατυπωθεί με στόχο να τηρηθούν ασφαλή ή να γίνουν ασφαλέστερα τα προσωπικά δεδομένα που κυκλοφορούν στο Διαδίκτυο και τα ΜΚΔ, να μην συλλέγονται και να μην χρησιμοποιούνται από άλλους –όποιοι κι αν είναι αυτοί– χωρίς την σαφή συγκατάθεση των χρηστών. Στο πλαίσιο προτάσεων και λύσεων, ιδιαίτερης σημασίας κρίνεται διαχρονικά η ενίσχυση της νομοθεσίας με στόχο ο τεχνολογικός σχεδιασμός της συλλογής στοιχείων και ο έλεγχος των αποκτούμενων στοιχείων να ρυθμιστεί (Buschel, Mehdi, Cammilleri, Marzouki, & Elger 2014). Στο πλαίσιο αυτό, η Οδηγία της Ευρωπαϊκής Ένωσης, το 1995 (95/46/EE), για την Προστασία των Δεδομένων αναμορφώθηκε από την Ευρωπαϊκή Επιτροπή το 2012 και η Επιτροπή πρότεινε το «δικαίωμα στη λήθη» (right to be forgotten), το «δικαίωμα στην ιδιωτικότητα από προεπιλογή» (privacy by default) και το «δικαίωμα στην ιδιωτικότητα από σχεδιασμό» (privacy by design), με στόχο να ενισχυθεί η προστασία της ιδιωτικότητας (Cecere, Le Guel & Soulié 2015). Ο νέος Κανονισμός, όπως εξηγήθηκε αναλυτικά στο πρώτο Κεφάλαιο, ενίσχυσε περαιτέρω τα δικαιώματα των υποκειμένων των δεδομένων, καθορίζοντας παράλληλα αυστηρές διαδικασίες για φορείς και οργανισμούς που συλλέγουν και επεξεργάζονται τέτοια δεδομένα.

3.3 Οι απόψεις των υποκειμένων των δεδομένων για τη νομοθεσία και το ρόλο της

Σύμφωνα με τους Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer & Lind (2015) η εγγραμματοσύνη της ιδιωτικότητας είναι ο συνδυασμός αφενός της γνώσης που έχουν τα υποκείμενα για τις τεχνικές όψεις της προστασίας των δεδομένων τους, τους σχετικούς νόμους και τις οδηγίες και αφετέρου της ικανότητάς τους να χρησιμοποιούν στρατηγικές για τη ρύθμιση της ιδιωτικότητάς τους και την προστασία των δεδομένων τους. Μάλιστα, οι ίδιοι εντάσσουν στην έξι διατάσεων Κλίμακα της Εγγραμματοσύνης για την Ψηφιακή Ιδιωτικότητα (Online Privacy Literacy Scale -OPLIS) τη διάσταση της γνώσης σχετικά με τις πρακτικές των οργανισμών και των παρόχων υπηρεσιών (διάσταση 1), εξηγώντας ότι καθώς τα υποκείμενα χρησιμοποιούν στην καθημερινότητά τους μια σειρά υπηρεσιών (πλατφόρμες, ιστότοπους, ψηφιακές κοινότητες) που για την τελική παροχή υπηρεσίας επιβάλλουν την αποκάλυψη προσωπικών δεδομένων, τα υποκείμενα οφείλουν να γνωρίζουν πώς οι πάροχοι χειρίζονται και αξιοποιούν αυτά (Trepte et al. 2015). Σύμφωνα με τον Park (2011) η γνώση των τεχνικών πτυχών και των θεσμικών πρακτικών συλλογής και χρησιμοποίησης δεδομένων μπορεί να βοηθήσει τα υποκείμενα να αναλάβουν τα κατάλληλα μέτρα. Ως τέταρτη διάσταση στην κλίμακα οι Trepte κ.α. (2015) εντάσσουν την γνώση για τη νομοθεσία, τις νομικές όψεις της προστασίας δεδομένων και τις πολιτικές προστασίας. Σημειώνουν δε ότι μόνο αν τα υποκείμενα των δεδομένων γνωρίζουν τα προσωπικά τους τα δικαιώματα και τους νομικούς περιορισμούς που επιβάλλονται στις εταιρείες μπορούν να λάβουν τεκμηριωμένες αποφάσεις και να ελέγξουν ή να βελτιστοποιήσουν την ιδιωτικότητά τους.

Η γνώση που έχουν τα υποκείμενα για τα δικαιώματά τους και την νομοθεσία έχει ήδη μελετηθεί. Η εργασία των Trepte κ.α. (2015) είναι ένα τέτοιο παράδειγμα με αναφορά στους Γερμανούς. Η έρευνα των Miltgen και Peyrat-Guillard (2014) εστίασε σε απόψεις για το ρόλο της νομοθεσίας και των δημοσίων Αρχών. Σύμφωνα με την έρευνα αυτή, οι Έλληνες συμμετέχοντες βλέπουν τις Αρχές ως μέσο προστασίας και τη νομοθεσία ως εκείνη που καθορίζει δικαιώματα και υποχρεώσεις όλων των πλευρών, ενώ οι Γάλλοι δείχνουν σκεπτικισμό στο αν πραγματικά η υφιστάμενη νομοθεσία λειτουργεί. Οι ερευνητές εξηγούν ότι η διαφορετική οπτική προκύπτει από τον συλλογικό ή ατομικιστικό χαρακτήρα του πολιτισμού. Η ερμηνεία αυτή συνάδει με τη θέση των Posey,

Lowry, Roberts & Ellis (2010) ότι στους πολιτισμούς που διακρίνονται από συλλογικότητα, τα υποκείμενα εμπιστεύονται περισσότερο τους άλλους. Στην ίδια έρευνα, οι Miltgen και Peyrat-Guillard (2014) έδειξαν ότι οι νέοι έχουν μεγαλύτερη εμπιστοσύνη, σε σχέση με τους μεγαλύτερους, στην προστασία από το νόμο, αλλά και στην ικανότητά τους να προστατεύσουν τον εαυτό τους. Σε άλλη έρευνα της Ευρωπαϊκής Επιτροπής (European Commission/Eurobarometer 2015), με αφορμή την καταγραφή ότι οι περισσότεροι από τους συμμετέχοντες στην έρευνα δεν διαβάζουν τις πολιτικές απορρήτου, διαπιστώθηκε ότι 14% εξ αυτών πιστεύουν ότι ο νόμος τους προστατεύει ούτως ή άλλως. Μάλιστα σε τρεις χώρες, πάνω από το 1/5 των συμμετεχόντων δήλωσε ότι δεν διαβάζει τις πολιτικές προστασίας γιατί θεωρεί ότι έχει την προστασία του νόμου: Αυστρία (24%), Δανία (21%) και Γερμανία (21%).

Αν και σε αρκετές περιπτώσεις τα υποκείμενα των δεδομένων αναγνωρίζουν το ρόλο των εταιρειών στη συλλογή και επεξεργασία των στοιχείων τους, σε κάποιες περιπτώσεις πιστεύουν πως οι εταιρείες φροντίζουν για την ασφάλειά τους. Η έρευνα, για παράδειγμα, των Kelley, Cranor & Sadeh (2013) έδειξε πως οι συμμετέχοντες που ανέφεραν πως δεν ανησυχούν γενικά για το διαμοιρασμό των δεδομένων τους, είχαν την πεποίθηση ότι οι εταιρείες τηρούν τους νόμους και οι ίδιες φροντίζουν για την ασφάλειά τους ως πελάτες.

Κεφάλαιο 4

Μεθοδολογία Έρευνας

Ο ΓΚΠΔ θέτει ένα νέο πλαίσιο με αναφορά στην προστασία των δεδομένων των υποκειμένων εισάγοντας ρυθμίσεις για τη συλλογή, επεξεργασία και διαχείρισή τους από φορείς, εταιρείες, οργανισμούς, καθορίζοντας, παράλληλα, αυστηρές κυρώσεις για όσους παραβαίνουν τις ρυθμίσεις αυτές και κυρίως διασφαλίζοντας τα δικαιώματα των ατόμων. Η εφαρμογή του στα κράτη μέλη της Ε.Ε. είναι πολύ πρόσφατη και μέχρι σήμερα έχουν δημοσιοποιηθεί μερικά στοιχεία σε σχέση με περιπτώσεις παραπόνων υποκειμένων δεδομένων που χειρίστηκαν οι Αρχές Προστασίας Δεδομένων και με πρόστιμα που επιβλήθηκαν για παραβάσεις. Συγκεκριμένα, στο διάστημα 5/2018-1/2019, οι Αρχές Προστασίας Δεδομένων επεξεργάστηκαν και ανταποκρίθηκαν σε 95.180 αιτήσεις παραπόνων για παραβίαση δεδομένων που υποβλήθηκαν, οι περισσότερες εκ των οποίων αφορούσαν προώθηση προϊόντων (telemarketing), διαφημιστικά e-mails και χρήση κάμερας για επιτήρηση, ενώ διερεύνησαν και 255 διακρατικές υποθέσεις².

Αν και είναι γνωστή η κάλυψη που έλαβε η εφαρμογή του ΓΚΠΔ από τα μέσα ενημέρωσης, αλλά και το ενδιαφέρον των πολιτών για το θέμα, όπως προκύπτει από αποτελέσματα αναζήτησης σε γνωστές μηχανές αναζήτησης, σύμφωνα με πρόσφατα στοιχεία της Ε.Ε³, μέχρι στιγμής, στο βαθμό που μας είναι γνωστό, δεν υπάρχουν επαρκή ερευνητικά στοιχεία για το βαθμό που τα υποκείμενα των δεδομένων γνωρίζουν τις θετικές ρυθμίσεις του ΓΚΠΔ για τα δικαιώματά τους.

² https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

³ https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

4.1 Δήλωση σκοπού έρευνας

Στο παραπάνω πλαίσιο, λοιπόν, έχει ενδιαφέρον να μελετηθεί η γνώση των υποκειμένων των δεδομένων για τη νέα νομοθεσία, τα δικαιώματα που τα ίδια έχουν και τις υποχρεώσεις των παρόχων υπηρεσιών, καθώς η διασφάλιση των προσωπικών δεδομένων οφείλει να απασχολεί ατομικά και συλλογικά. Επιπλέον, είναι ενδιαφέρον το πώς η γνώση αυτή δυνητικά επιδρά σε αντιλήψεις και συμπεριφορές τους σε σχέση με την ιδιωτικότητα και την προστασία των δεδομένων τους.

Η παρούσα διατριβή στοχεύει, λοιπόν, στη διερεύνηση της γνώσης ομάδας ενηλίκων χρηστών του Διαδικτύου και των ΜΚΔ σχετικά με τις ρυθμίσεις που φέρνει ο ΓΚΠΔ στο θέμα της συλλογής και διαχείρισης προσωπικών τους δεδομένων από οργανισμούς, εταιρείες ή παρόχους και των δικαιωμάτων που ως υποκείμενα των δεδομένων έχουν. Συγκεκριμένα, στόχος είναι να εξεταστεί αν οι χρήστες, ένα χρόνο μετά την εφαρμογή του Κανονισμού, γνωρίζουν τη νέα νομοθεσία και σε ποιο βαθμό κατανοούν τις προβλέψεις- δικαιώματα που θεσπίζονται γι' αυτούς. Σε δεύτερο επίπεδο, ανιχνεύονται αντιλήψεις σε σχέση με τον έλεγχο της πληροφορίας, τις ανησυχίες ιδιωτικότητας και τη συμπεριφορά των χρηστών.

Ειδικότερα, η έρευνα που έχει το χαρακτήρα της διερευνητικής (exploratory research) (Research Methodology 2013) εστιάζει σε επιμέρους ζητήματα και συγκεκριμένα στη διερεύνηση :

- Του βαθμού της γνώσης των υποκειμένων των δεδομένων σε σχέση με τα δικαιώματα που θεσπίζει ο ΓΚΠΔ
- Του εκτιμώμενου ελέγχου επί των προσωπικών τους δεδομένων
- Των εκτιμώμενων κινδύνων σε σχέση με τα προσωπικά δεδομένα
- Της συμπεριφοράς προστασίας των προσωπικών δεδομένων

Στο παραπάνω πλαίσιο, με βάση τη θέση των Trepte κ.α. (2015) ότι, αν τα υποκείμενα των δεδομένων γνωρίζουν τα προσωπικά τους τα δικαιώματα και τους νομικούς περιορισμούς που επιβάλλονται στις εταιρείες, μπορούν να λάβουν τεκμηριωμένες αποφάσεις και να ελέγξουν ή να βελτιστοποιήσουν την ιδιωτικότητά τους, διατυπώνεται η βασική ερευνητική υπόθεση: *Ο υψηλός βαθμός γνώσης των δικαιωμάτων των*

υποκειμένων, όπως καταγράφονται στον ΓΚΠΔ, αυξάνει τις ανησυχίες ιδιωτικότητας και επιδρά θετικά στη συμπεριφορά προστασίας προσωπικών δεδομένων.

4.2 Οργάνωση Ερευνητικής Διαδικασίας

Από τα πρώτα στάδια μιας έρευνας, οι ερευνητές/τριες αποφασίζουν για μια σειρά θεμάτων που αφορούν το δείγμα και τη μέθοδο επιλογής αυτού καθώς και το ερευνητικό εργαλείο που θα χρησιμοποιηθεί (Cohen & Manion, 1994).

4.2.1. Επιλογή δείγματος

Δεδομένου ότι ο δυνητικός πληθυσμός της έρευνας (ενήλικοι, χρήστες του Διαδικτύου και των ΜΚΔ) είναι μεγάλος, στην παρούσα έρευνα επελέγη δείγμα ευκολίας (availability sample) (Ζαφειρόπουλος 2015). Η συγκεκριμένη δειγματοληπτική μέθοδος αξιοποιείται σε περιπτώσεις όπου οι συνθήκες της έρευνας (χρόνος, κόστος κλπ) δεν επιτρέπουν την επιλογή αντιπροσωπευτικού δείγματος και ουσιαστικά ο ερευνητής επιλέγει για το δείγμα του άτομα που δέχονται να συμμετάσχουν στην έρευνα. Το γεγονός αυτό, αν και δεν επιτρέπει την γενίκευση των αποτελεσμάτων της έρευνας, ωστόσο μπορεί να αναδείξει τάσεις για μελλοντική ευρύτερη έρευνα.

4.2.2. Ερευνητικό Εργαλείο

Ως εργαλείο συλλογής δεδομένων χρησιμοποιήθηκε, το ερωτηματολόγιο, που αποτελεί εύχρηστο μέσο συλλογής πληροφορίας, εύκολο στην ανάλυσή του, καθώς δομείται στη βάση συγκεκριμένων εννοιολογικών κατηγοριών που θέτει ο ερευνητής/τρια, γεγονός που συμβάλλει στην τυποποίηση της ανάλυσης και ως εκ τούτου στην ευκολότερη εξαγωγή συμπερασμάτων, ενώ παράλληλα η συμπλήρωσή του δεν απαιτεί ιδιαίτερα πολύ χρόνο σε αντίθεση π.χ. με τις συνεντεύξεις. Η έρευνα διεξήχθη στο διάστημα από 18/3/2019 έως και 18/4/2019.

Κατά τη σχεδίαση του δομημένου ερωτηματολογίου ακολουθήθηκαν βασικοί κανόνες σύνταξης (Javeau 1996) :

- Δόθηκε τίτλος στην αρχή του ερωτηματολογίου, ακολούθησε το εισαγωγικό σημείωμα και τα στοιχεία της έρευνας.
- Το ερωτηματολόγιο οργανώθηκε σε ενότητες που εξετάζουν συγκεκριμένες μεταβλητές και περιλαμβάνουν ομοειδείς ερωτήσεις.

- Οι ερωτήσεις αριθμήθηκαν ανά ενότητα.
- Οι ερωτήσεις δεν υπαγορεύουν την απάντηση, έτσι ώστε ο/η ερωτώμενος/η να έχει τη δυνατότητα απάντησης βάσει της δικής του άποψης.

Με βάση το πλαίσιο της ανάλυσης που προκύπτει από την μελέτη ιδίως του ΓΚΠΔ, αλλά και βιβλιογραφίας σχετικής με τον νέο Κανονισμό, καθορίστηκαν οι υπό εξέταση μεταβλητές, για τις οποίες έπρεπε να συλλεγούν πληροφορίες και σχεδιάστηκε το ερωτηματολόγιο της έρευνας⁴ αποτελούμενο από κλειστού τύπου ερωτήσεις (δικοτομικές, διαβαθμισμένης κλίμακας [κλίμακα Likert], απλής και πολλαπλής επιλογής), ενταγμένες σε τέσσερις (4) ενότητες με διαφορετικό τίτλο η καθεμία, ανταποκρινόμενο στο περιεχόμενο των ερωτήσεων. Ερωτήσεις των Ενότητων (Α) και (Γ) αντλήθηκαν από προηγούμενη έρευνα (European Commission/Eurobarometer 2015). Γι' αυτές γίνεται αναλυτικά λόγος στο πέμπτο κεφάλαιο.

Οι συμμετέχοντες/ουσες στην έρευνα ενημερώθηκαν με σαφήνεια για το σκοπό της έρευνας, σύμφωνα με τους κανόνες της ερευνητικής διαδικασίας (Babbie 2011), διαβεβαιούμενοι/ες για την ανωνυμία των απαντήσεών τους. Σκοπός της ανωνυμίας είναι η προστασία της εμπιστευτικότητας της έρευνας που μαζί με την πληροφορημένη συναίνεση συνιστούν ζητήματα ηθικής και δεοντολογίας της έρευνας.

Η δομή του ερωτηματολογίου έχει ως ακολούθως :

Ενότητα Α: Γενικός Κανονισμός Προστασίας Δεδομένων.

Στην ενότητα αυτή περιλαμβάνονται 4 ερωτήσεις που διερευνούν γενικά θέματα, όπως τον τρόπο πληροφόρησης των ερωτώμενων για τον ΓΚΠΔ και τον στόχο της νέας νομοθεσίας.

Ενότητα Β : Τα δικαιώματα των υποκειμένων των δεδομένων

Στην ενότητα αυτή περιλαμβάνονται 14 ερωτήσεις που διερευνούν το βαθμό της γνώσης των ερωτώμενων σε σχέση με τα δικαιώματα που προβλέπονται στον ΓΚΠΔ (πχ. δικαίωμα ενημέρωσης, διαγραφής, διόρθωσης δεδομένων, συγκατάθεση).

Ενότητα Γ. Κίνδυνοι για τα προσωπικά δεδομένα και τρόποι προστασίας

Η ενότητα αυτή χωρίζεται σε δύο (2) υποενότητες. Η πρώτη (Έλεγχος προσωπικών δεδομένων και κίνδυνοι) περιλαμβάνει 10 ερωτήσεις που εστιάζουν στον εκτιμώμενο

⁴ Βλ. Παράρτημα Β.

έλεγχο των ερωτώμενων για τα προσωπικά τους δεδομένα, σε ανησυχίες ιδιωτικότητας και σε θεωρούμενους κινδύνους για τα προσωπικά δεδομένα. Η δεύτερη υποενότητα (*Προστασία προσωπικών δεδομένων*) περιλαμβάνει 7 ερωτήσεις που διερευνούν τη συμπεριφορά των ερωτώμενων σε σχέση με τις δηλώσεις απορρήτου, την παροχή συγκατάθεσης, τη γνώση για τη συλλογή και επεξεργασία των πληροφοριών τους.

Ενότητα Δ : Ατομικές Πληροφορίες

Οι τέσσερις (4) ερωτήσεις της ενότητας αυτής καταγράφουν δημογραφικά και κοινωνικά χαρακτηριστικά των ερωτώμενων (φύλο, ηλικία, μορφωτικό επίπεδο, επάγγελμα).

Για να υπολογιστεί η αξιοπιστία της κλίμακας που αφορά στη γνώση των δικαιωμάτων των υποκειμένων των δεδομένων (ενότητα Β ερωτηματολογίου) χρησιμοποιήθηκε ο δείκτης αξιοπιστίας Cronbach's Alpha ($\alpha=0,847$). Ο ίδιος δείκτης χρησιμοποιήθηκε και για την κλίμακα ανησυχιών ιδιωτικότητας (υποενότητα Γ.1 ερωτηματολογίου) ($\alpha=0,808$).

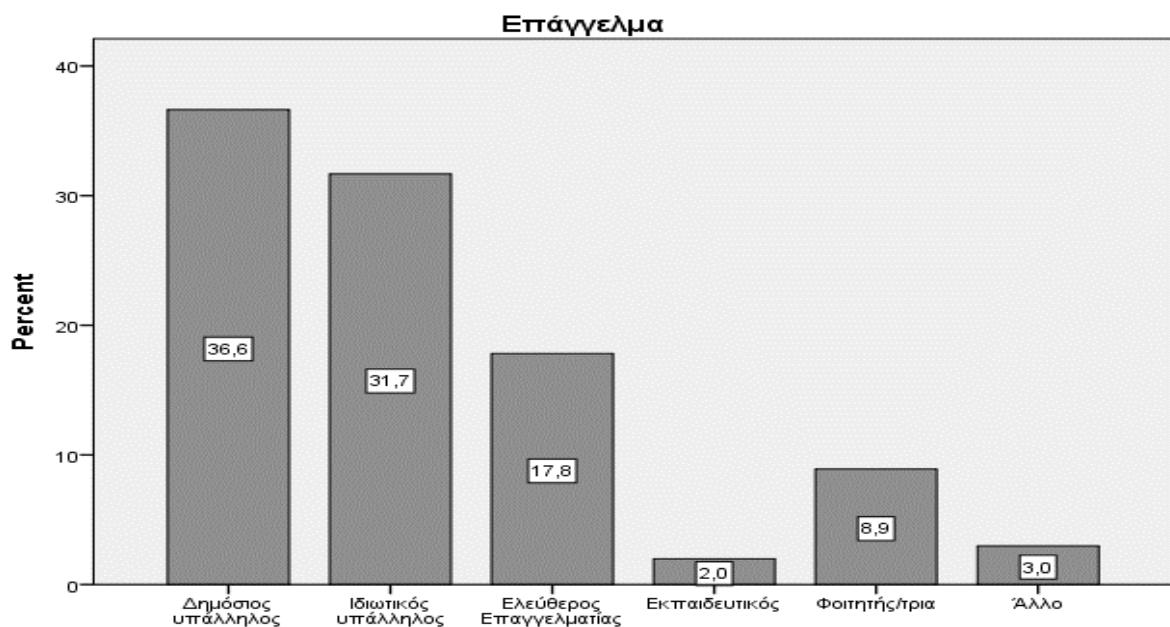
Μετά την σύνταξή του, το ερωτηματολόγιο ελέγχθηκε ως προς τη μορφή του, τη γλώσσα του, τη σαφήνεια του, τη δυσκολία και την αξιοπιστία του σε μια πιλοτική έρευνα που προηγήθηκε της κύριας δειγματοληψίας. Η δοκιμαστική έρευνα είναι ένα σημαντικό στάδιο (Orpenheim1992) καθώς επιδιώκει να ανιχνεύσει: α) αν οι ερωτήσεις γίνονται κατανοητές, β) αν η κάθε ερώτηση εξασφαλίζει την πληροφορία για την οποία σχεδιάστηκε και γ) αν διασφαλίζει το ενδιαφέρον και τη συνεργασία των ερωτώμενων. Μετά την παραπάνω δοκιμαστική έρευνα, το ερωτηματολόγιο διορθώθηκε και έλαβε την οριστική του μορφή.

Το ερωτηματολόγιο δημιουργήθηκε με το εργαλείο Google forms (<https://goo.gl/forms/QNIci5AjUD1DZike2>) και τα δεδομένα που συλλέχθηκαν από την έρευνα αναλύθηκαν με το πρόγραμμα IBM SPSS Statistics 21.

Κεφάλαιο 5

Αποτελέσματα Έρευνας

Στην έρευνα⁵ που υλοποιήθηκε για την παρούσα μεταπτυχιακή διατριβή, στο χρονικό διάστημα από 18/3/2019-18/4/2019, συμμετείχαν 49 άνδρες και 51 γυναίκες (ένας/μια εκ των ερωτώμενων δεν δήλωσε φύλο). Το μεγαλύτερο ποσοστό των συμμετεχόντων ανήκει στην ηλικιακή ομάδα 36-45 ετών (49.5%), έπεται αυτό της ομάδας 26-35 ετών (25.7%) και ακολουθούν με μικρότερα ποσοστά οι έχοντες ηλικία 46-55 ετών (15.8%), 18-25 ετών (5.9%) και >56 ετών (3%). Το μεγαλύτερο ποσοστό είναι κάτοχοι μεταπτυχιακού τίτλου σπουδών (42.6%) και έπονται οι απόφοιτοι Πανεπιστημίου (38.6%). Μικρότερο είναι το ποσοστό των αποφοίτων Λυκείου (15.8%) και των κατόχων διδακτορικού τίτλου (3%). Η επαγγελματική απασχόληση των συμμετεχόντων εμφανίζεται στο ακόλουθο διάγραμμα.

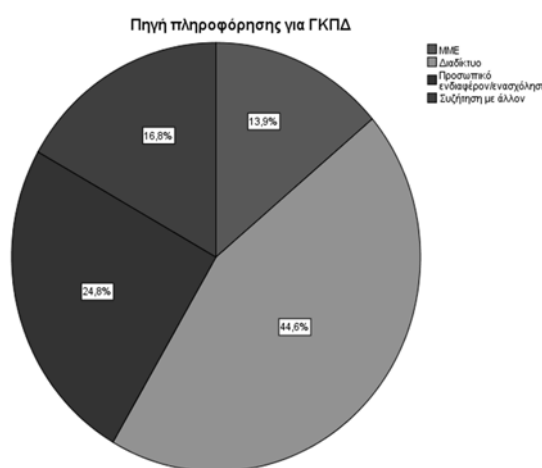


Διάγραμμα 1. Επαγγελματική απασχόληση των συμμετεχόντων στην έρευνα

⁵ Πίνακες αποτελεσμάτων περιλαμβάνονται στο Παράρτημα Γ.

5.1. Ενότητα Α «Γενικός Κανονισμός Προστασίας Δεδομένων»

Σχεδόν οι μισοί από τους ερωτηθέντες είχαν πληροφόρηση για τον ΓΚΠΔ από το Διαδίκτυο (44.6%), ενώ το ποσοστό όσων έμαθαν για τον νέο Κανονισμό από τα ΜΜΕ ήταν 13.9%, πραγματικότητα που προκύπτει καθώς το Διαδίκτυο αποτελεί την πιο άμεση πηγή πληροφόρησης. Ενδιαφέρον παρουσιάζει ότι 24.8% των συμμετεχόντων έχουν γνώση για τον Κανονισμό από προσωπική ενασχόληση/ενδιαφέρον, γεγονός που μάλλον συνάδει με τις ανησυχίες των χρηστών για την ασφάλεια των προσωπικών τους δεδομένων και την ανάγκη τους να πληροφορηθούν τρόπους προστασίας τους. Τέλος, όπως φαίνεται από τα αποτελέσματα, το θέμα του νέου Κανονισμού συζητάται μεταξύ των χρηστών, καθώς η πληροφόρηση από τη συζήτηση με κάποιον άλλο εμφανίζεται με ποσοστό 16.8%.



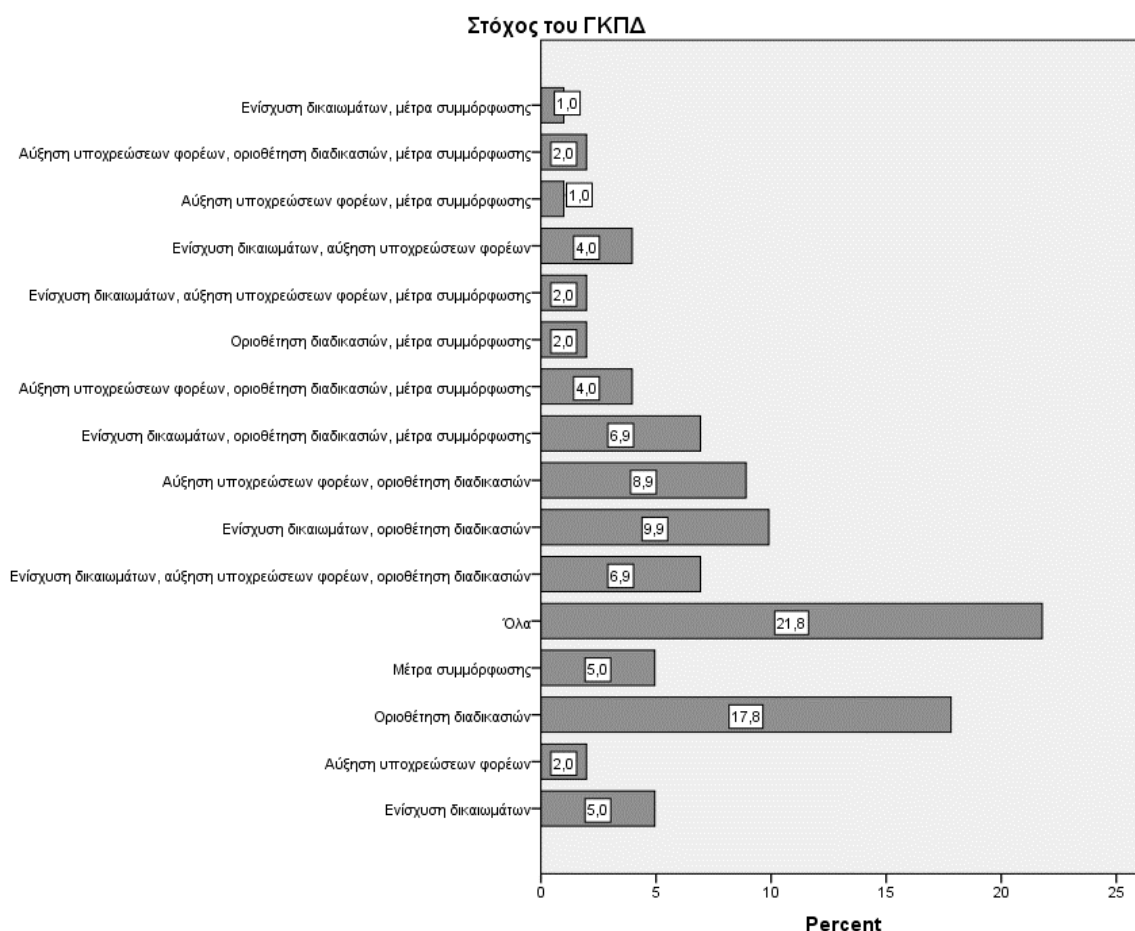
Διάγραμμα 2. Πηγή πληροφόρησης για ΓΚΠΔ

Η συντριπτική πλειοψηφία των χρηστών (82.2%) αναγνώρισε ότι η εφαρμογή του ΓΚΠΔ αποτελεί ευθύνη σε επίπεδο Ευρωπαϊκής Ένωσης και μόνο 6,9% σε επίπεδο εθνικό. Ωστόσο, διαπιστώθηκε ότι σχεδόν 10% των ερωτηθέντων δεν γνωρίζει ποιος έχει την ευθύνη εφαρμογής.

Άγνοια σε ποσοστό ιδιαίτερα υψηλό (41.6%) εμφανίστηκε στην ερώτηση αν γνωρίζουν οι συμμετέχοντες ποια είναι η Αρμόδια Ρυθμιστική Αρχή στην Ελλάδα που είναι υπεύθυνη για την προστασία των δικαιωμάτων τους αναφορικά με τα προσωπικά δεδομένα. Αντίθετα, θετική απάντηση δόθηκε από 58.4%. Στην αντίστοιχη ερώτηση της έρευνας του 2015 (European Commission/Eurobarometer 2015), 56% των Ελλήνων ερωτώμενων δήλωσε πως γνώριζε την Αρχή και 44% όχι (στην Ευρώπη τα αντίστοιχα ποσοστά ήταν 37% «ναι» 61% «όχι»), γεγονός που δηλώνει μικρή μεταβολή των ποσοστών από το 2015, αν και τα αποτελέσματα της παρούσας έρευνας δεν μπορούν να γενικευθούν σε επίπεδο πληθυσμού. Η άγνοια που καταγράφηκε κυρίως στην ερώτηση

που αφορούσε την Αρμόδια Ρυθμιστική Αρχή αποτελεί ένδειξη ότι, σε υψηλό βαθμό, οι χρήστες δεν γνωρίζουν ποιος δύναται να τους προστατεύσει.

Προκειμένου να εκτιμηθεί σε πρώτο επίπεδο η γνώση που έχουν οι ερωτώμενοι για τον ΓΚΠΔ, τέθηκε η ερώτηση «Σε ποια από τα παρακάτω ζητήματα θεωρείτε ότι ανταποκρίνεται ο ΓΚΠΔ;» και δόθηκε η δυνατότητα για συνδυασμό απαντήσεων. Ουσιαστικά στόχος της ερώτησης ήταν να διερευνηθεί αν οι ερωτώμενοι γνωρίζουν το στόχο του ΓΚΠΔ. Σύμφωνα με το Άρθρο 1 αυτού «1. Ο παρών κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα [...] 2. Ο παρών κανονισμός προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα». Με άλλα λόγια ο ΓΚΠΔ στοχεύει κυρίως στην ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων.

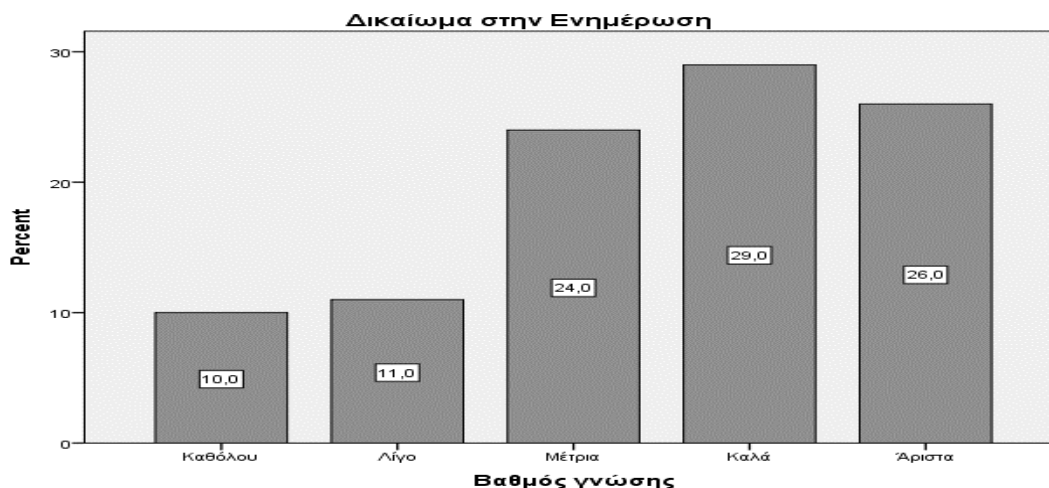


Διάγραμμα 3. Αντίληψη των ερωτώμενων για το στόχο του ΓΚΠΔ

Τα αποτελέσματα στη συγκεκριμένη ερώτηση, όπως παρουσιάζονται στο Διάγραμμα 3, δείχνουν ότι οι ερωτώμενοι σε ποσοστό 21.8% δηλώνουν ότι ανταποκρίνεται στο σύνολο των απαντήσεων που προτάθηκαν, γεγονός που υποδεικνύει ότι κατανοούν τόσο το στόχο του ΓΚΠΔ όσο και τον τρόπο που αυτός επιτυγχάνεται, με την αύξηση δηλαδή των υποχρεώσεων των φορέων που συλλέγουν και διαχειρίζονται δεδομένα, την αυστηρότερη οριοθέτηση των διαδικασιών συλλογής και επεξεργασίας δεδομένων και την θέσπιση αυστηρότερων μέτρων ελέγχου συμμόρφωσης με τη νομοθεσία. Σε ποσοστό 17.8% εμφανίστηκε ως μοναδική επιλογή η αυστηρότερη οριοθέτηση των διαδικασιών συλλογής και επεξεργασίας δεδομένων, ακολουθούμενη από την ενίσχυση των δικαιωμάτων των χρηστών και την θέσπιση αυστηρότερων μέτρων ελέγχου συμμόρφωσης με τη νομοθεσία (5% και στις δύο περιπτώσεις). Με χαμηλότερο ποσοστό (ως μοναδική απάντηση) καταγράφηκε η αύξηση των υποχρεώσεων των φορέων (2%), ενώ παράλληλα τα αποτελέσματα καταδεικνύουν και συνδυασμούς απαντήσεων. Μεμονωμένα η εξέταση των απαντήσεων καταδεικνύει ότι ελάχιστα περισσότεροι από τους μισούς ερωτώμενους αντιλαμβάνονται ότι ο ΓΚΠΔ στοχεύει στην ενίσχυση των δικαιωμάτων τους και στην αύξηση των υποχρεώσεων των φορέων (N=58 και N=53 αντίστοιχα), 46 στη θέσπιση μέτρων ελέγχου συμμόρφωσης με τη νομοθεσία, ενώ η πλειονότητα (N=81) στην αυστηρότερη οριοθέτηση διαδικασιών. Τα στοιχεία αυτά δείχνουν ότι οι ερωτώμενοι δίνουν μεγαλύτερη έμφαση σε θέματα που άπτονται της λειτουργίας των φορέων που συλλέγουν και διαχειρίζονται δεδομένα και μικρότερη στην άσκηση από τους ίδιους των δικαιωμάτων τους.

5.2. Ενότητα Β «Τα δικαιώματα των υποκειμένων των δεδομένων»

Το δικαίωμα του υποκειμένου των δεδομένων στην ενημέρωση είναι θεμελιώδης αρχή στην διαδικασία επεξεργασίας προσωπικών δεδομένων. Για το βαθμό γνώσης του δικαιώματος αυτού (ερώτηση Β.1) κλήθηκαν να απαντήσουν οι ερωτώμενοι χρησιμοποιώντας μια πεντάβαθμη διαβαθμισμένη κλίμακα σημείων, όπου το (1) αναφέρεται στο καθόλου (απουσία γνώσης) και το (5) στο άριστα (άριστη γνώση). Η ίδια κλίμακα χρησιμοποιήθηκε και για τις υπόλοιπες ερωτήσεις της συγκεκριμένης ενότητας με εξαίρεση τις τελευταίες ερωτήσεις Β.13 και Β.14 (πολλαπλών απαντήσεων).



Διάγραμμα 4. Βαθμός γνώσης των ερωτώμενων για την υποχρέωση του διαχειριστή να ενημερώσει για την επεξεργασία στην οποία πρόκειται να υποβληθούν τα δεδομένα και για τα δικαιώματα του υποκειμένου

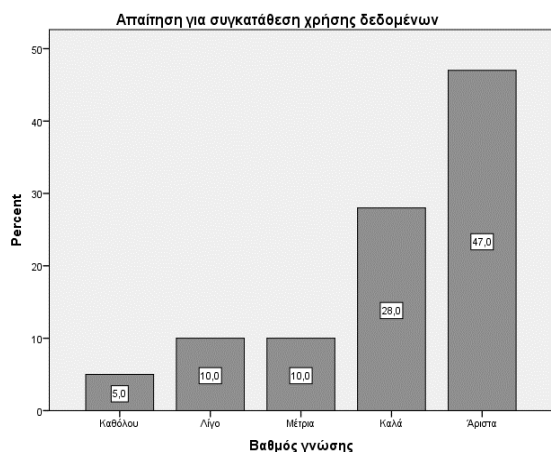
Όπως προκύπτει από το παραπάνω Διάγραμμα 4, πάνω από τους μισούς ερωτώμενους (55%) γνωρίζουν «άριστα» (26%) και «καλά» (29%) το δικαίωμά τους στην ενημέρωση. «Καθόλου» και «λίγο» δήλωσε αντίστοιχα 10% και 11%, ενώ «μέτρια» 24%.

Στην ερώτηση σε ποιο βαθμό γνωρίζουν το δικαίωμά τους να απαιτήσουν από τον υπεύθυνο επεξεργασίας, χωρίς αδικαιολόγητη καθυστέρηση, τη διόρθωση ανακριβών προσωπικών τους δεδομένων (B.2), «άριστα» απάντησε 19.2% των ερωτώμενων και «καλά» 27.3%. Καθόλου δεν γνωρίζει το δικαίωμα αυτό 11.1%, ενώ ίδιο ποσοστό δήλωσε «λίγο». Όπως και στην προηγούμενη ερώτηση (B.1) παρατηρείται ένα ποσοστό περίπου 20% που είτε δεν γνωρίζει καθόλου ή γνωρίζει ελάχιστα το δικαίωμα αυτό. Η επιλογή «μέτρια» εκφράστηκε από 31.3% των συμμετεχόντων.

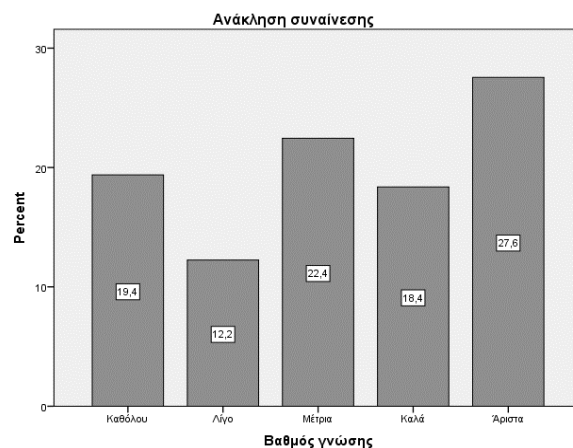
Οι ερωτήσεις B.3 έως B.6 αφορούν τη συγκατάθεση του υποκειμένου που είναι απαιτητά για την διαδικασία επεξεργασίας των δεδομένων του.

Τα αποτελέσματα των απαντήσεων στην ερώτηση B.3 (Διάγραμμα 5) που αφορά αν γνωρίζουν οι ερωτώμενοι ότι για τη χρήση των προσωπικών τους δεδομένων απαιτείται η συγκατατάθεσή τους δείχνουν ότι σχεδόν οι μισοί (47%) γνωρίζουν άριστα το δικαίωμα αυτό. «Καλά» δήλωσε 28%, «μέτρια» 10%, το ίδιο ποσοστό «λίγο» και μόνο 5% «καθόλου». Τα στοιχεία αυτά δείχνουν ότι οι ερωτώμενοι έχουν υψηλότερο βαθμό

γνώσης για την απαίτηση αυτή (προϋπόθεση χρήσης δεδομένων τους) από ό,τι για το δικαίωμα στην ενημέρωση και το δικαίωμα στη διόρθωση. Μάλιστα, όπως προκύπτει από την ερώτηση Β.4 που αφορά στη μορφή που πρέπει να έχει η συγκατάθεση, αθροιστικά ποσοστό 60,4% των ερωτώμενων γνωρίζει «άριστα» (23.8%) και «καλά» (36.6%) ότι η συγκατάθεση πρέπει να είναι ελεύθερη, συγκεκριμένη και ρητή. «Μέτρια» γνωρίζει αυτό 23.8%, «λίγο» όπως και «καθόλου» 7.9% των ερωτώμενων.



Διάγραμμα 5. Βαθμός γνώσης των ερωτώμενων για απαίτηση συγκατάθεσης χρήσης δεδομένων του

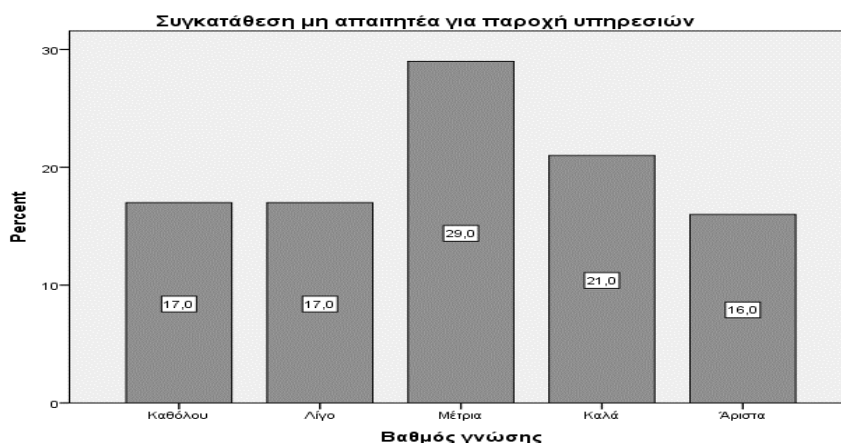


Διάγραμμα 6. Βαθμός γνώσης των ερωτώμενων για δικαίωμα ανάκλησης συγκατάθεσης

Αν και αθροιστικά το ποσοστό των ερωτώμενων που γνωρίζουν «άριστα» (47%) και «καλά» (28%) το γεγονός ότι η συγκατάθεση είναι απαιτητέα για την επεξεργασία των δεδομένων τους είναι ικανοποιητικό (75%), το αντίστοιχο αθροιστικό ποσοστό όσων έχουν «άριστο» (27.6%) και «καλό» (18.4%) βαθμό γνώσης του δικαιώματος ανάκλησης της συγκατάθεσης οποιαδήποτε στιγμή υπολείπεται αρκετά (46%), όπως προέκυψε από τις απαντήσεις στην ερώτηση Β.5 (Διάγραμμα 6). Λαμβάνοντας δε υπόψη ότι 19.4% δεν γνωρίζει καθόλου το δικαίωμα αυτό, 12.2% «λίγο» και 22.4% «μέτρια», γίνεται αντιληπτό ότι οι ερωτώμενοι θεωρούν ότι από τη στιγμή που συναινούν στην επεξεργασία των δεδομένων τους, δεν έχουν ή έχουν ελάχιστη δυνατότητα να μεταστρέψουν την συναίνεσή τους.

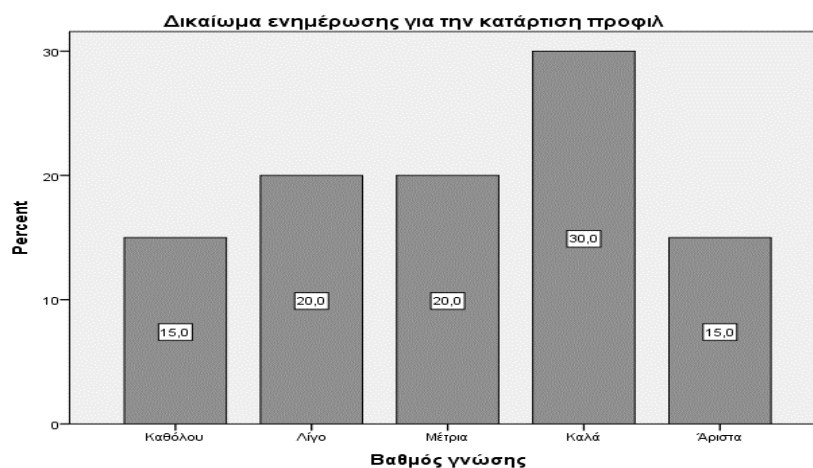
Συχνά οι χρήστες θεωρούν ότι η συγκατάθεσή τους είναι μάλλον προϋπόθεση για την παροχή υπηρεσιών. Η Rouillet (2018), μάλιστα, διατύπωσε τη θέση ότι η συγκατάθεση που παρέχεται από τα υποκείμενα των δεδομένων γίνεται μια εσφαλμένη προϋπόθεση μπροστά σε συγκεκριμένες κοινωνικές ανάγκες όπως η πρόσβαση στο Διαδίκτυο ή σε υπηρεσίες όπως οι μηχανές αναζήτησης και τα κοινωνικά δίκτυα. Τα αποτελέσματα της

ερώτησης Β.6 «Σε ποιο βαθμό γνωρίζετε ότι η συγκατάθεση δεν είναι προϋπόθεση για την παροχή υπηρεσιών, εκτός αν η χρήση δεδομένων είναι απαραίτητη για την παροχή της υπηρεσίας;» (Διάγραμμα 7) δείχνουν ότι 34% των ερωτώμενων δήλωσε ότι δεν γνωρίζει αυτό «καθόλου» (17%) ή το γνωρίζει «λίγο» (17%). Αντίθετα, 29% γνωρίζει αυτό «μέτρια», 21% «καλά» και 16% «άριστα». Τα αποτελέσματα αυτά είναι μάλλον ενθαρρυντικά, καθώς δείχνουν ότι σταδιακά οι χρήστες αντιλαμβάνονται πως η συγκατάθεσή τους δεν είναι προϋπόθεση ώστε να τους παράσχεται μια υπηρεσία.



Διάγραμμα 7. Βαθμός γνώσης των ερωτώμενων για συγκατάθεση μη απαιτητέα για παροχή υπηρεσιών

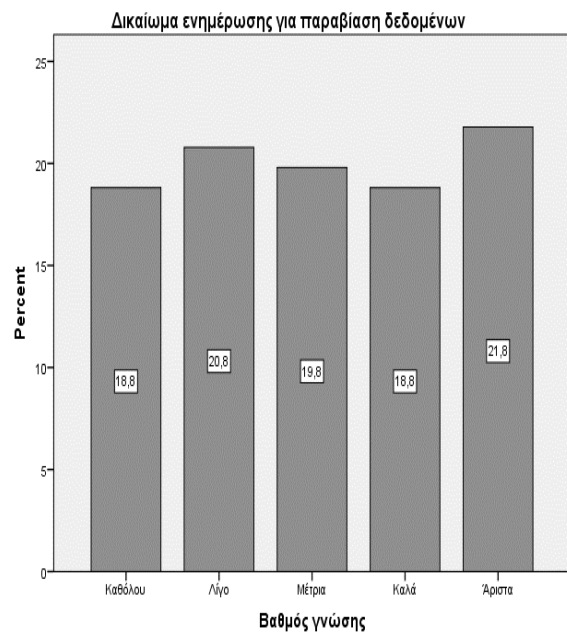
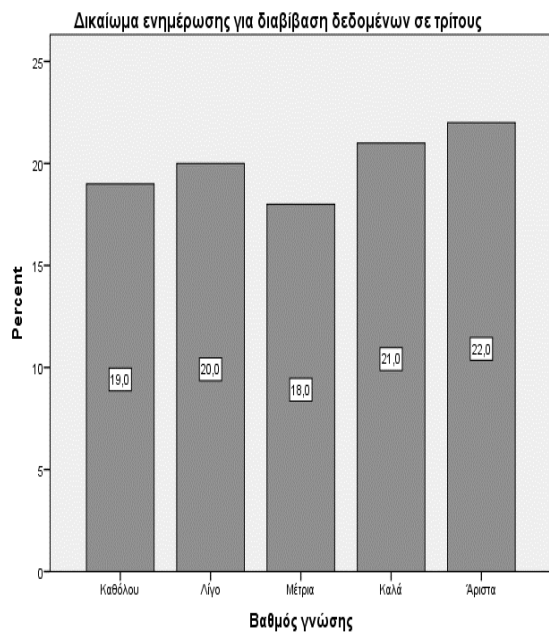
Το θέμα της κατάρτισης προφίλ αναφέρεται σε τουλάχιστον τρία άρθρα του ΓΚΠΔ, τα άρθρα 13, 15 και 22. Όπως προκύπτει από τα αποτελέσματα της ερώτησης Β.7 (Διάγραμμα 8) που αφορά στο βαθμό που τα υποκείμενα των δεδομένων γνωρίζουν ότι, σε περίπτωση χρήσης των δεδομένων τους για την κατάρτιση προφίλ, πρέπει να προηγείται ενημέρωση προς αυτά και για τη διαδικασία και για τις συνέπειές της, μόνο 15% των ερωτώμενων δήλωσαν ότι δεν έχουν γνώση αυτής της υποχρέωσης του διαχειριστή των δεδομένων τους. «Άριστα» και «καλά» δήλωσαν αντίστοιχα 15% και 30% των ερωτώμενων, «μέτρια» όπως και «λίγο» 20%. Τα δεδομένα αυτά δείχνουν μερική ευαισθητοποίηση των χρηστών σε σχέση με το θέμα της κατάρτισης προφίλ.



Διάγραμμα 8. Βαθμός γνώσης των ερωτώμενων για δικαίωμα ενημέρωσης σε περίπτωση κατάρτισης προφιλ

Οι χρήστες έχουν συχνά ανησυχία για το σε ποιόν μπορεί να διαβιβαστούν τα δεδομένα τους. Στο πλαίσιο αυτό, ο ΓΚΠΔ ορίζει ότι σε περίπτωση που τα δεδομένα διαβιβαστούν σε τρίτους, ο διαχειριστής οφείλει να ενημερώσει το αργότερο μετά την πρώτη διαβίβαση. Στην ερώτηση Β.8 διερευνήθηκε ο βαθμός γνώσης των υποκειμένων σε σχέση με τη συγκεκριμένη υποχρέωση του διαχειριστή (Διάγραμμα 9). Τα αποτελέσματα δείχνουν μια σχεδόν ισότιμη κατανομή μεταξύ των απαντήσεων «καθόλου», «λίγο», «μέτρια», «καλά» και «άριστα» (19%, 20%, 18%, 21% και 22% αντίστοιχα), γεγονός που μάλλον προβληματίζει καθώς θα αναμένετο, δεδομένων των ανησυχιών των χρηστών, να γνωρίζουν καλά την συγκεκριμένη υποχρέωση του διαχειριστή.

Αντίστοιχα, ανάλογη ισότιμη κατανομή απαντήσεων εμφανίζεται και στην ερώτηση Β.9 (Διάγραμμα 10) «Σε ποιο βαθμό γνωρίζετε ότι όταν δεδομένα προσωπικού χαρακτήρα υψηλού κινδύνου παραβιαστούν, ο υπεύθυνος επεξεργασίας υποχρεούται να σας ενημερώσει για την παραβίαση, τις συνέπειες και τα μέτρα που λαμβάνει;». Όπως προκύπτει από το Διάγραμμα 10, 18,8%, 20,8%, 19,8%, 18,8% και 21,8% απάντησαν «καθόλου», «λίγο», «μέτρια», «καλά» και «άριστα» αντίστοιχα. Παρά το γεγονός, λοιπόν, ότι τα υποκείμενα των δεδομένων ανησυχούν για ενδεχόμενες παραβιάσεις αυτών και τις δυνητικές τους συνέπειες, δεν φαίνεται να γνωρίζουν σε ικανοποιητικό βαθμό την υποχρέωση του διαχειριστή να τα ενημερώσει.

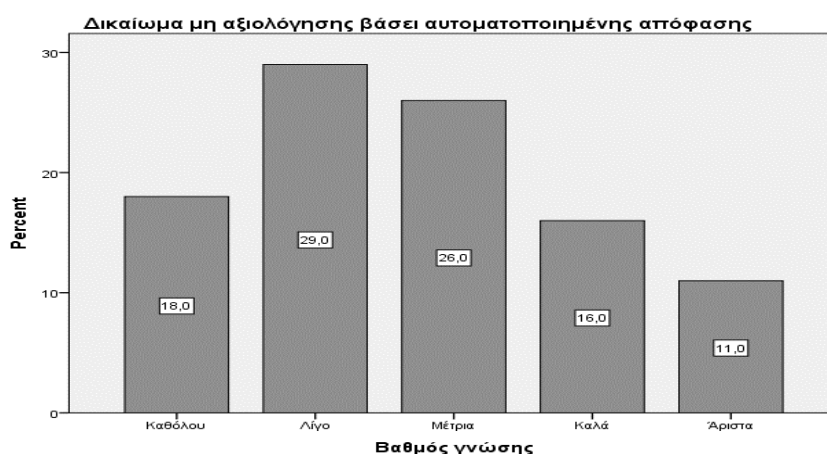


Διάγραμμα 9. Βαθμός γνώσης των ερωτώμενων για δικαίωμα ενημέρωσης σε περίπτωση διαβίβασης δεδομένων σε τρίτους

Διάγραμμα 10. Βαθμός γνώσης των ερωτώμενων για δικαίωμα ενημέρωσης σε περίπτωση παραβίασης δεδομένων

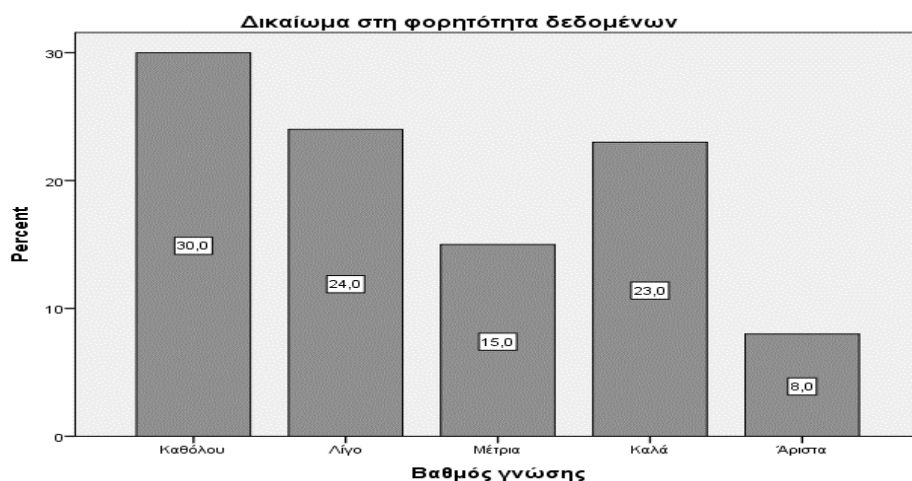
Στην ερώτηση Β.10, διερευνήθηκε ο βαθμός γνώσης των υποκειμένων σε σχέση με το δικαίωμα να αντιτάσσονται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή τους, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα (επεξεργασία από δημόσιες αρχές ή από ιδιώτες), περιλαμβανομένης της κατάρτισης προφίλ. Τα ευρήματα από τις απαντήσεις δείχνουν ότι «άριστα» και «καλά» γνωρίζουν το δικαίωμα αυτό 14% και 24% αντίστοιχα, «καθόλου» και «λίγο» 14% και 26% αντίστοιχα και «μετρίως» 22%. Τα δεδομένα αυτά δημιουργούν προβληματισμό σε σχέση με το αν τα υποκείμενα θα αξιοποιήσουν το δικαίωμα αυτό. Η Pouillet (2018) σημειώνει, βέβαια, ότι η ρύθμιση του συγκεκριμένου δικαιώματος δεν είναι ικανοποιητική για την αποτελεσματική προστασία του υποκειμένου των δεδομένων, καθώς δεν αρκεί το υποκείμενο που ανακαλύπτει ότι έχει υποβληθεί σε κατάρτιση προφίλ να υποβάλλει αίτηση, ώστε αυτό να μην ξανασυμβεί ή να ενίσταται στην απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας. Αυτό που ενδιαφέρει το υποκείμενο των δεδομένων, όπως εξηγεί η Pouillet είναι να κατανοήσει τα κριτήρια που λαμβάνονται υπόψη για το προφίλ, δηλαδή να υπάρχει διαφάνεια σχετικά με τον αλγόριθμο που οδήγησε στο αποτέλεσμα αυτό και με τα δεδομένα που τηρούνται.

Με αναφορά στην ερώτηση Β.11 «Σε ποιο βαθμό γνωρίζετε ότι έχετε το δικαίωμα να μην υπόκεισθε σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, με την οποία αξιολογούνται προσωπικές πτυχές που σας αφορούν και παράγονται αποτελέσματα που σας επηρεάζουν (πχ. έννομα αποτελέσματα);», τα ευρήματα από τις απαντήσεις (Διάγραμμα 11) δείχνουν ότι 47% των ερωτώμενων δεν γνωρίζουν (18%) ή γνωρίζουν «λίγο» (29%) το δικαίωμα αυτό. Οι απαντήσεις «άριστα» και «καλά» δηλώθηκαν από 11% και 16% αντίστοιχα, ενώ μέτρια απάντησε 26%. Ο ΓΚΠΔ δίνει το δικαίωμα για εξήγηση των αλγορίθμων, αλλά αυτό υλοποιείται μόνο εκ των προτέρων με μια αναφορά στην λειτουργικότητα του συστήματος κι όχι εκ των υστέρων που θα σήμαινε ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερωθεί σχετικά με τη λογική και τα κριτήρια της συγκεκριμένης απόφασης (van Ooijen & Vrabec 2019).



Διάγραμμα 11. Βαθμός γνώσης των ερωτώμενων για δικαίωμα να αντιταχθούν σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας

Το δικαίωμα στη φορητότητα εισήχθη με τον ΓΚΠΔ και θεωρείται ότι αυξάνει τον έλεγχο των χρηστών στη διαχείριση των δεδομένων τους. Η ερώτηση Β.12 αφορά στο βαθμό που τα υποκείμενα των δεδομένων γνωρίζουν ότι έχουν το δικαίωμα να λάβουν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και έχουν παρασχεθεί σε υπεύθυνο επεξεργασίας και να τα διαβιβάσουν σε άλλον υπεύθυνο επεξεργασίας. Το Διάγραμμα 12 δείχνει ότι το 1/3 των ερωτώμενων (30%) δεν γνωρίζει «καθόλου» το δικαίωμα αυτό και 24% το γνωρίζει «λίγο». Πολύ χαμηλό, μόλις 8%, είναι το ποσοστό όσων γνωρίζουν το δικαίωμα «άριστα». Οι απαντήσεις «καλά» και «μέτρια» δηλώθηκαν από 23% και 15% των ερωτώμενων αντίστοιχα.



Διάγραμμα 12. Βαθμός γνώσης των ερωτώμενων για δικαίωμα στη φορητότητα δεδομένων

Συγκρίνοντας τους Μ.Ο. του βαθμού γνώσης των χρηστών (Πίνακες 1-3) σε σχέση με τα δικαιώματά τους, όπως διερευνήθηκαν στις ερωτήσεις B.1-B.12, συνάγεται ότι οι χρήστες έχουν υψηλότερο βαθμό επίγνωσης για την απαίτηση της συγκατάθεσης προκειμένου να χρησιμοποιηθούν τα δεδομένα τους (Μ.Ο 4.02), όπως και για τη μορφή της συγκατάθεσης που πρέπει να είναι ελεύθερη, συγκεκριμένη και ρητή (Μ.Ο 3.6). Σχετικά ικανοποιητικός εμφανίζεται ο βαθμός γνώσης για το δικαίωμα στην ενημέρωση (υποχρέωση του διαχειριστή να ενημερώσει το υποκείμενο των δεδομένων για τον τρόπο επεξεργασίας των δεδομένων του) (Μ.Ο. 3.5), όπως και για το δικαίωμα στη διόρθωση ανακριβών δεδομένων (Μ.Ο. 3.32). Αντιθέτως, οριακός εμφανίζεται ο βαθμός της γνώσης των υποκειμένων για το δικαίωμα στη φορητότητα (Μ.Ο. 2.55) και το δικαίωμα να μην υπόκεινται σε απόφαση που λαμβάνεται αποκλειστικά στη βάση αυτοματοποιημένης επεξεργασίας (Μ.Ο. 2.73).

	Right_inform_pr ocess	Right_correct_in accurate_data	Consensus_requi red_for_data_pro cess	Consensus_speci fic_explicit
N Valid	100	99	100	101
N Missing	1	2	1	0
Mean	3,5000	3,3232	4,0200	3,6040
Mode	4,00	3,00	5,00	4,00

Πίνακας 1. Μ.Ο βαθμού γνώσης των ερωτώμενων για δικαιώματα (ερωτήσεις B.1-B.4)

		Consensus_recal led	Consensus_not_r equired_for_serv ice_usage	Right_inform_pr ofilling	Right_inform_da ta_transmission
N	Valid	98	100	100	100
	Missing	3	1	1	1
Mean		3,2245	3,0200	3,1000	3,0700
Mode		5,00	3,00	4,00	5,00

Πίνακας 2. Μ.Ο βαθμού γνώσης των ερωτώμενων για δικαιώματα (ερωτήσεις B.5-B.8)

		Right_inform_da ta_breach	Right_oppose_da ta_process	Right_not_subjec t_automated_des icion	Right_transport_ data_other_proc essor
N	Valid	101	100	100	100
	Missing	0	1	1	1
Mean		3,0396	2,9800	2,7300	2,5500
Mode		5,00	2,00	2,00	1,00

Πίνακας 3. Μ.Ο βαθμού γνώσης των ερωτώμενων για δικαιώματα (ερωτήσεις B.8-B.12)

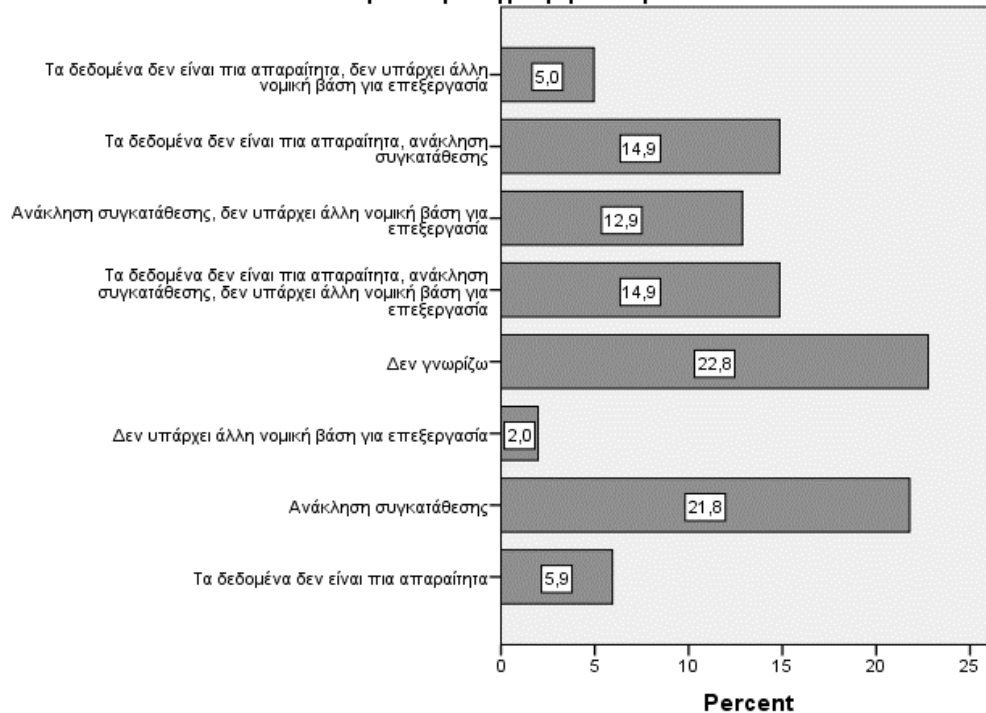
N	Valid	101
	Missing	0
Mean		37,7525
Median		39,0000
Mode		36,00
Minimum		12,00
Maximum		60,00

Πίνακας 4. Μ.Ο βαθμού γνώσης των ερωτώμενων για σύνολο δικαιωμάτων

Όπως προκύπτει από τον Πίνακα 4, η ελάχιστη και μέγιστη τιμή βαθμού γνώσης που εμφανίστηκε για το σύνολο των δικαιωμάτων είναι αντίστοιχα 12 και 60, με δεσπόζουσα τιμή 36 (N=8) και Μ.Ο 37,75.

Οι προϋποθέσεις για την άσκηση του δικαιώματος στη διαγραφή των δεδομένων, γνωστό ως δικαίωμα στη λήθη, αναφέρεται στο άρθρο 17 του ΓΚΠΔ.

Δικαίωμα στη διαγραφή δεδομένων

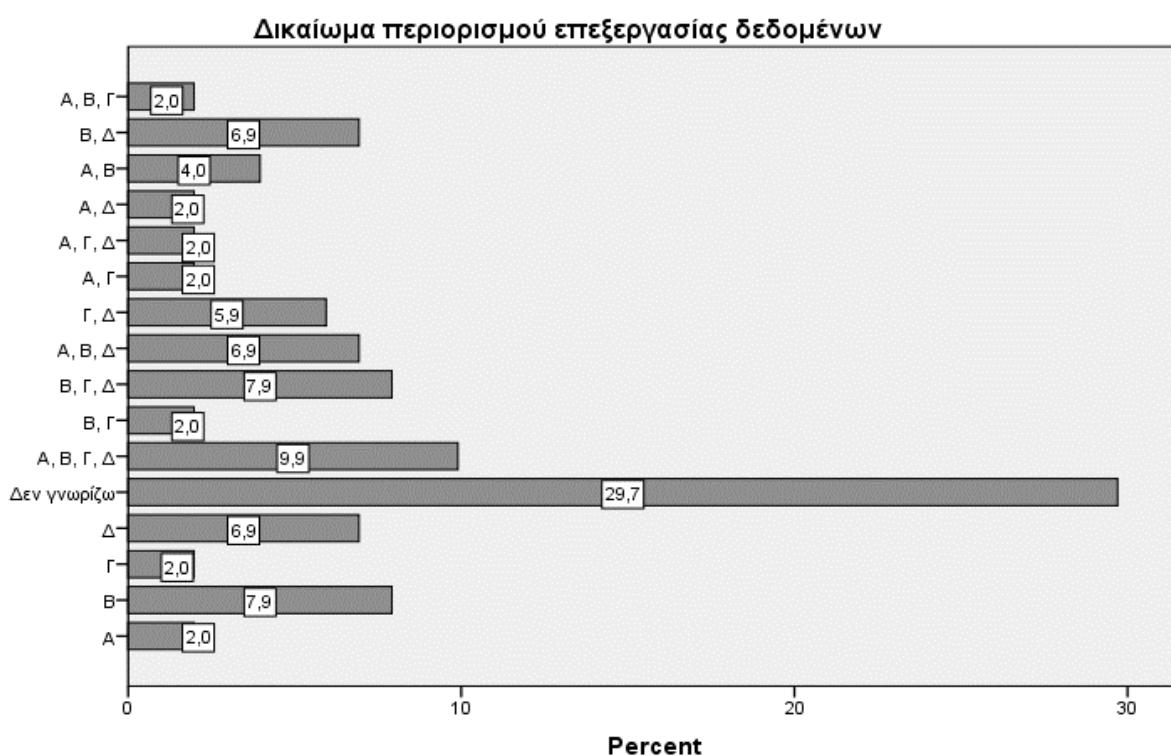


Διάγραμμα 13. Βαθμός γνώσης των ερωτώμενων για προϋποθέσεις άσκησης δικαιώματος στη λήθη

Από τα αποτελέσματα της ερώτησης B.13 προκύπτει (Διάγραμμα 13) ότι περίπου 1/5 των ερωτώμενων δεν γνωρίζει σε ποιες περιπτώσεις έχει δικαίωμα να ζητήσει από τον υπεύθυνο της επεξεργασίας τη διαγραφή προσωπικών του δεδομένων, ενώ μόνο 14.9% αναγνωρίζει ότι έχει το δικαίωμα αυτό και στις τρεις δοθείσες περιπτώσεις. Με υψηλότερο ποσοστό απαντήσεων 21.8% εμφανίζεται η περίπτωση της ανάκλησης της συγκατάθεσης ως προϋπόθεση του αιτήματος διαγραφής προσωπικών δεδομένων, ενώ παράλληλα καταγράφεται και ένας συνδυασμός απαντήσεων με χαμηλότερα ποσοστά. Μεμονωμένη καταγραφή των απαντήσεων καταδεικνύει ότι 65 από τους ερωτηθέντες δήλωσαν ότι έχουν δικαίωμα να ζητήσουν διαγραφή των προσωπικών τους δεδομένων όταν ανακαλέσουν τη συγκατάθεσή τους, 41 όταν τα δεδομένα δεν είναι πλέον απαραίτητα και 35 όταν δεν υπάρχει πλέον νομική βάση για την επεξεργασία τους.

Στην ερώτηση B.14 διερευνήθηκε η γνώση των υποκειμένων για τις περιπτώσεις που έχουν το δικαίωμα να ζητήσουν τον περιορισμό της επεξεργασίας των δεδομένων τους αυτές (Διάγραμμα 14), όπως προβλέπονται στο άρθρο 18 του ΓΚΠΔ. Τα αποτελέσματα της έρευνας δείχνουν ότι σχεδόν το 1/3 των ερωτώμενων (29.7%) δεν γνωρίζει σε ποιες περιπτώσεις έχει δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας των προσωπικών του δεδομένων, ενώ μόνο 9.9% αναγνωρίζει ότι έχει το δικαίωμα αυτό και

στις τέσσερις δοθείσες περιπτώσεις. Αυτό είναι και το υψηλότερο ποσοστό που εμφανίζεται συγκριτικά με άλλες απαντήσεις (συνδυασμός περιπτώσεων). Η μεμονωμένη καταγραφή των απαντήσεων καταδεικνύει ότι 49 από τους ερωτηθέντες δήλωσαν ότι έχουν δικαίωμα να ζητήσουν περιορισμό της επεξεργασίας των προσωπικών τους δεδομένων όταν «έχουν αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερισχύουν έναντι όλων των δικών τους λόγων», 48 όταν «η επεξεργασία είναι παράνομη», ενώ πολύ λιγότεροι απάντησαν «όταν η ακρίβεια των δεδομένων αμφισβητείται» ή «όταν ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο για την θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων» (N=31 και N=34 αντίστοιχα).



A. Όταν η ακρίβεια των δεδομένων αμφισβητείται, Β. Όταν η επεξεργασία είναι παράνομη, Γ. Όταν ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από εσάς για την θεμελίωση, την άσκηση ή την υποστήριξη νομικών, Δ. Όταν έχετε αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερισχύουν έναντι όλων των δικών σας λόγων

Διάγραμμα 14. Βαθμός γνώσης των ερωτώμενων για προϋποθέσεις άσκησης δικαιώματος περιορισμού επεξεργασίας δεδομένων.

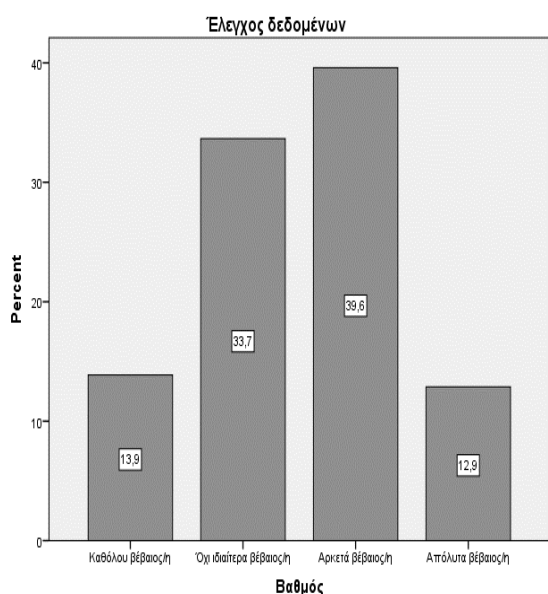
5.3. Ενότητα Γ, υποενότητα Γ.1 «Έλεγχος Προσωπικών Δεδομένων και Κίνδυνοι»

Όπως ήδη εξηγήθηκε, στόχος του ΓΚΠΔ είναι η ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων. Ωστόσο δεν αρκεί τα υποκείμενα να έχουν γνώση των δικαιωμάτων τους, αλλά να έχουν και επίγνωση του τρόπου που τα ίδια ή άλλοι διαχειρίζονται τα δεδομένα τους και των κινδύνων που προκύπτουν δυνητικά από τη διαχείριση αυτή. Οι 10 ερωτήσεις της υποενότητας Γ.1 του ερωτηματολογίου στοχεύουν στη διερεύνηση του βαθμού ελέγχου των δεδομένων των υποκειμένων, των ανησυχιών ιδιωτικότητας και της αντίληψης κινδύνων για τα προσωπικά τους δεδομένα.

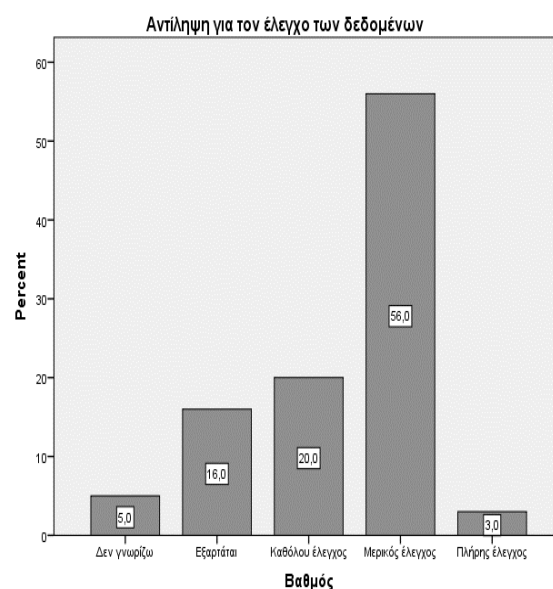
Στην ερώτηση Γ.1.1, οι ερωτώμενοι κλήθηκαν να δηλώσουν αν ελέγχουν τα προσωπικά δεδομένα που παρέχουν online. Οι van Ooijen & Vrabec (2019: 93) ορίζουν τον ατομικό έλεγχο ως «το βαθμό στον οποίο ένα άτομο έχει συνείδηση μιας κατάστασης και τη συνειδητή πρόθεση και τη δυνατότητα να ξεκινήσει, να σταματήσει ή να διατηρήσει μια κατάσταση». Η αντίληψη του ελέγχου είναι κρίσιμη, δεδομένου ότι μπορεί να οδηγήσει είτε σε αίσθημα ασφάλειας και, συνεπώς, σε μεγαλύτερη αποκάλυψη πληροφοριών, είτε σε υψηλές ανησυχίες για την προστασία της ιδιωτικής ζωής και σε μείωση της προθυμίας αποκάλυψης, ακόμη και σε περιπτώσεις που οι κίνδυνοι από τη δημοσιοποίηση είναι μικρότεροι (Brandimarte, Acquisti & Loewenstein, 2012). Τα ευρήματα από τις απαντήσεις των ερωτώμενων (Διάγραμμα 15) δείχνουν ότι 12.9% είναι απόλυτα βέβαιοι ότι ελέγχουν τα προσωπικά δεδομένα που παρέχουν online και 39.6% ότι είναι αρκετά βέβαιοι.

Ωστόσο, στην επόμενη ερώτηση (Γ.1.2) «Κατά πόσον νιώθετε ότι έχετε τον έλεγχο της πληροφορίας που παρέχετε online; (π.χ. την δυνατότητα να διορθώσετε, να αλλάξετε ή και να διαγράψετε αυτήν την πληροφορία;)), μόνο 3% των ερωτώμενων δήλωσαν ότι έχουν πλήρη έλεγχο. Πάνω από τους μισούς ερωτώμενους (56%) δήλωσαν ότι έχουν μερικό και 20% ότι δεν έχουν κανένα έλεγχο. Σε προηγούμενη έρευνα (European Commission/Eurobarometer 2015) τα αντίστοιχα ποσοστά ήταν 31%, 46% και 22% (με Μ.Ο Ευρώπης 15% «πλήρης έλεγχος», 50% «μερικός έλεγχος» και 31% «καθόλου έλεγχος»). Με μικρότερα ποσοστά, όπως φαίνεται στο Διάγραμμα 16, εμφανίστηκαν οι απαντήσεις «δεν γνωρίζω» και «εξαρτάται» (5% και 16% αντίστοιχα). Αν και κάποιος θα μπορούσε να θεωρήσει ότι υπάρχει αναντιστοιχία μεταξύ των απαντήσεων της

ερώτησης Γ.1.1 και Γ.1.2, η διαφοροποίηση προκύπτει από τη διάκριση μεταξύ της πράξης της ανάρτησης και αυτής της πρόσβασης άλλων στην πληροφορία και της χρήσης της πληροφορίας. Οι Brandimarte κ.α. (2012) εξηγούν ότι πρέπει να γίνει διαχωρισμός ανάμεσα στην πράξη της αποκάλυψης πληροφορίας, στην πράξη της πρόσβασης και στην πράξη της χρήσης ή κατάχρησης της πληροφορίας, δίνοντας έτσι έμφαση στο γεγονός ότι το προκύπτον κόστος εξαρτάται από την πρόσβαση και χρήση/κατάχρηση της πληροφορίας, πράγμα που οι άνθρωποι αποτυγχάνουν να σκεφτούν, καθώς εστιάζουν στο πρώτο επίπεδο ελέγχου (απελευθέρωση πληροφορίας). Στην περίπτωση μας, οι ερωτώμενοι κατόρθωσαν να διακρίνουν μεταξύ του ελέγχου που έχουν σε επίπεδο κοινοποίησης των δεδομένων και του ελέγχου που έχουν μερικώς ή δεν έχουν σε επίπεδο πρόσβασης, αλλαγής ή διαγραφής της πληροφορίας τους.



Διάγραμμα 15. Βαθμός βεβαιότητας ελέγχου προσωπικών δεδομένων που παρέχονται online



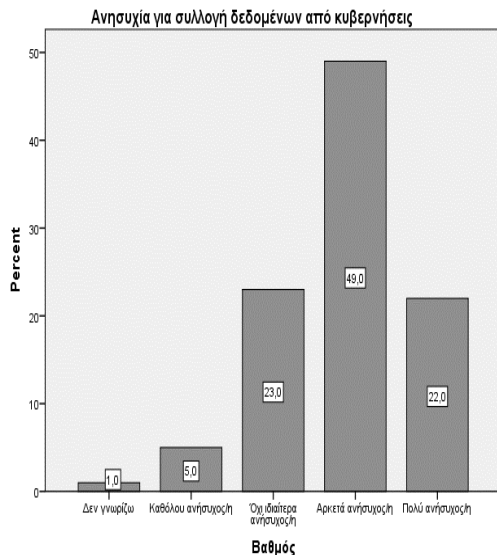
Διάγραμμα 16. Βαθμός ελέγχου των πληροφοριών που παρέχονται online

Οι ερωτήσεις Γ.1.3-Γ.1.7 επικεντρώθηκαν στην ανίχνευση ανησυχιών και προβληματισμών των ερωτώμενων. Συγκεκριμένα, στην ερώτηση Γ.1.3 ζητήθηκε από τους ερωτώμενους να καταγράψουν πόσο ανησυχούν για το γεγονός ότι κάποιος άλλος ελέγχει την πληροφορία τους. Τα αποτελέσματα δείχνουν ότι με εξαίρεση 2% των ερωτώμενων που απάντησε «καθόλου» και 14.9% που δήλωσε όχι ιδιαίτερη ανησυχία, 82.2% δήλωσε «πολύ ανήσυχος» (14.9%) και «αρκετά ανήσυχος» (67.3%). Μόνο 1% απάντησε «δεν γνωρίζω». Τα στοιχεία αυτά καταδεικνύουν υψηλά επίπεδα ανησυχίας για τον έλεγχο των προσωπικών πληροφοριών από άλλους, ενισχύοντας τα ευρήματα της ερώτησης Γ.1.2. Στην έρευνα του 2015 (European Commission/Eurobarometer

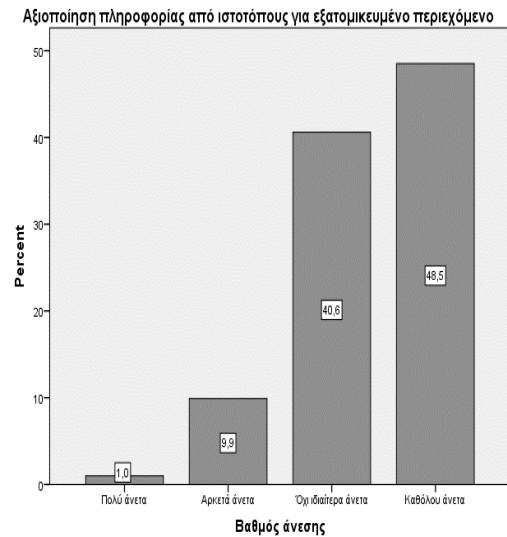
2015) σε επίπεδο Ελλήνων ερωτώμενων, τα ποσοστά για τις απαντήσεις «πολύ ανήσυχος», «αρκετά ανήσυχος», «όχι ιδιαίτερα ανήσυχος» και καθόλου ανήσυχος» ήταν αντίστοιχα 25%, 47%, 24% και 4% (αντίστοιχοι Μ.Ο. Ευρώπης 18%, 49%, 28% και 4%).

Οι ανησυχίες για την ιδιωτικότητα και την ασφάλεια των δεδομένων ολοένα αυξάνονται, καθώς κυβερνήσεις και ιδιωτικοί φορείς (πχ. εταιρείες) συγκεντρώνουν προσωπικά δεδομένα. Στην ερώτηση Γ.1.4, οι ερωτώμενοι κλήθηκαν να απαντήσουν σε ποιο βαθμό τους ανησυχούν οι αποκαλύψεις ότι κυβερνητικοί φορείς συλλέγουν προσωπικά δεδομένα σε μεγάλη κλίμακα με σκοπό την εθνική ασφάλεια. Το Διάγραμμα 17 δείχνει ότι 49% των ερωτώμενων είναι αρκετά ανήσυχτοι και 22% πολύ ανήσυχτοι, ενώ μόλις 5% δεν δηλώνουν καμία ανησυχία και 23% όχι ιδιαίτερη ανησυχία. Στην πανευρωπαϊκή έρευνα του 2015 (European Commission/Eurobarometer 2015) οι Έλληνες ερωτώμενοι που γνώριζαν ότι οι κυβερνήσεις συλλέγουν δεδομένα για λόγους εθνικής ασφάλειας δήλωσαν, για την επίδραση που έχει αυτό στην εμπιστοσύνη τους στις κυβερνήσεις, θετική επίδραση (20%), αρνητική (48%) καμία επίδραση (29%). Η εθνική ασφάλεια και η προστασία των πολιτών είναι ένας από τους λόγους που οι χρήστες αποδέχονται την απεμπόληση του δικαιώματος στην ιδιωτικότητα. Σε έρευνα που έγινε το 2017, από την YouGov, σχετικά με τη χρήση του Διαδικτύου δείχνοντας υψηλά ποσοστά ανησυχιών για το έγκλημα στον κυβερνοχώρο και τις κυβερνοεπιθέσεις, διαπιστώθηκε ότι 32% των ερωτώμενων πίστευε ότι πρέπει να γίνουν περισσότερα για την καταπολέμηση του εγκλήματος με κόστος την ιδιωτικότητα (Bhaimia 2018).

Οι ανησυχίες των υποκειμένων των δεδομένων αυξήθηκαν σημαντικά όταν ρωτήθηκαν (Γ.1.5) πόσο άνετα νιώθουν με το γεγονός ότι οι ιστοσελίδες εταιρειών χρησιμοποιούν την πληροφορία για την online δραστηριότητά σας, ώστε να διαμορφώσουν περιεχόμενο που ανταποκρίνεται στις προτιμήσεις τους (πχ. προσωποποιημένες διαφημίσεις). Τα αποτελέσματα, όπως παρουσιάζονται στο Διάγραμμα 18, δείχνουν ότι αθροιστικά 89.1% των ερωτώμενων νιώθουν «όχι ιδιαίτερα άνετα» (40.6%) και καθόλου άνετα (48.5%). Μόνο 9.9% δήλωσε «αρκετά άνετα» και 1% «πολύ». Στην ίδια ερώτηση, η έρευνα του 2015 (European Commission/Eurobarometer 2015) έδειξε ότι στην Ελλάδα οι ερωτώμενοι ένιωθαν αρκετά άνετα (31%), όχι ιδιαίτερα άνετα (45%), καθόλου άνετα (18%) και πολύ άνετα (4%).

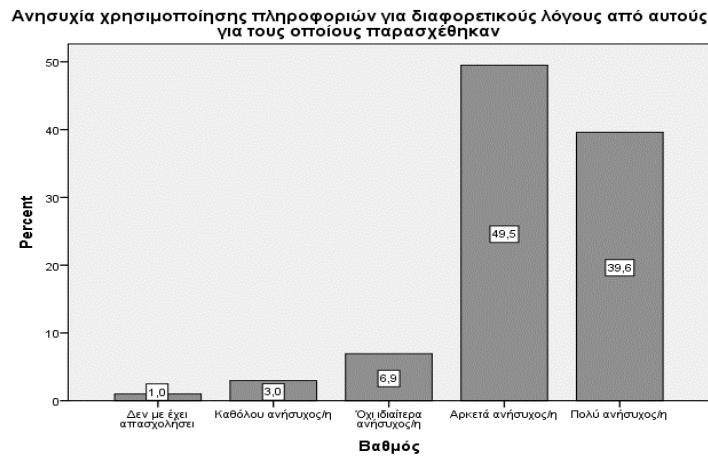


Διάγραμμα 17. Βαθμός ανησυχίας για συλλογή δεδομένων από κυβερνήσεις



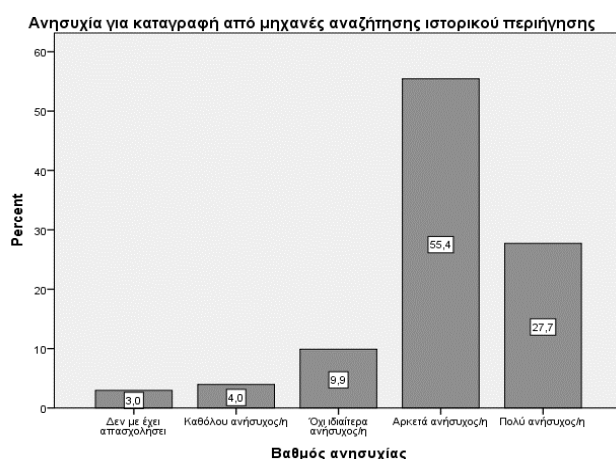
Διάγραμμα 18. Βαθμός άνεσης για αξιοποίηση προσωπικής πληροφορίας από εταιρείες με στόχο τη διαμόρφωση εξατομικευμένου περιεχομένου

Συχνά τα υποκείμενα των δεδομένων ανησυχούν μήπως πληροφορίες τους που έχουν συλλεγεί από δημόσιους ή ιδιωτικούς φορείς χρησιμοποιηθούν για διαφορετικούς λόγους από αυτούς για τους οποίους είχαν συλλεγεί αρχικά, χωρίς να ενημερωθούν. Οι ανησυχίες αυτές καταγράφηκαν και στην έρευνα του 2015 (European Commission/Eurobarometer 2015). Με αναφορά στα ευρήματα για την Ελλάδα, 22% των ερωτώμενων δήλωσαν πολύ ανήσυχος, 43% αρκετά ανήσυχος, 22% όχι ιδιαίτερα ανήσυχος και 7% καθόλου (Μ.Ο Ευρώπης 25%, 44%, 22%, 6%). Πολύ μικρά ήταν τα ποσοστά όσων επέλεξαν την απάντηση «Δεν ξέρω» (3% Μ.Ο Ευρώπης, 1% Ελλάδα). Τα αποτελέσματα των απαντήσεων που δόθηκαν στο πλαίσιο της παρούσας έρευνας στην ερώτηση Γ.1.6 (Διάγραμμα 19) δείχνουν ότι 39.6% των ερωτώμενων νιώθουν πολύ ανήσυχος και 49.5% αρκετά. Μόνο 3% δεν έχει καμία ανησυχία και 6.9% δήλωσε «όχι ιδιαίτερα ανήσυχος». Τέλος, 1% δήλωσε ότι το θέμα δεν τους έχει απασχολήσει. Αν και είναι δύσκολο να γίνει σύγκριση μεταξύ της παρούσας έρευνας και εκείνης του 2015, λόγω της φύσης της έρευνας (διερευνητική) και του δείγματος (δείγμα ευκολίας), ωστόσο θα μπορούσε να υποστηριχθεί μια τάση αύξησης των ανησυχιών στη βάση του γεγονότος ότι η πληθώρα περιστατικών που έχει ως σήμερα δημοσιοποιηθεί για διαρροή προσωπικών δεδομένων και χρήση τους για άλλους λόγους από εκείνους για τους οποίους παρασχέθηκαν (πχ. υπόθεση Cambridge Analytica) έχει ευαισθητοποιήσει τα υποκείμενα των δεδομένων.



Διάγραμμα 19. Βαθμός ανησυχίας για αξιοποίηση προσωπικής πληροφορίας για διαφορετικό λόγο από αυτόν για τον οποίο παρασχέθηκε

Η ερώτηση Γ.1.7 «Σε ποιο βαθμό σας προβληματίζει το γεγονός ότι δημοφιλείς μηχανές αναζήτησης, όπως η Google, καταγράφουν τις ιστοσελίδες από τις οποίες προήλθατε καθώς και αυτές τις οποίες επισκέπτεστε;» διερεύνησε την ανησυχία των υποκειμένων των δεδομένων σε σχέση με το θέμα της εποπτείας/επιτήρησης στα ψηφιακά περιβάλλοντα. Η φιλοσοφία του «Πανοπτικού» (ένα πλαίσιο επιτήρησης κρατουμένων που αναπτύχθηκε από τον Jeremy Bentham, στα τέλη του 18ου αιώνα) έχει επεκταθεί στον κυβερνοχώρο (Ragnedda 2011), περιλαμβάνοντας τον έλεγχο των κινήσεων των ανθρώπων στο Διαδίκτυο, την αξιολόγηση των συμπεριφορών, νοοτροπιών, στάσεων, δράσεων και ικανοτήτων που αναπτύσσουν (Van Dijck 2013). Τα αποτελέσματα των απαντήσεων των ερωτώμενων (Διάγραμμα 20) δείχνουν αυξημένες ανησυχίες.



Συγκεκριμένα, 27.7% δήλωσαν πολύ ανήσυχοι και 55.4% αρκετά. Καθόλου ανήσυχοι δήλωσε 4%, όχι ιδιαίτερα 9.9%, ενώ το θέμα δεν έχει απασχολήσει 3% των ερωτώμενων.

Διάγραμμα 20. Βαθμός ανησυχίας για καταγραφή ιστορικού περιήγησης από μηχανές αναζήτησης

Όπως φαίνεται στον Πίνακα 5 που ακολουθεί ο βαθμός ανησυχίας των υποκειμένων των δεδομένων για τα θέματα για τα οποία ερωτήθηκαν (Γ.1.3-Γ.1.7) είναι αρκετά υψηλός (Μ.Ο. 15.37) με ελάχιστη και μέγιστη τιμή αντίστοιχα 6 και 20.

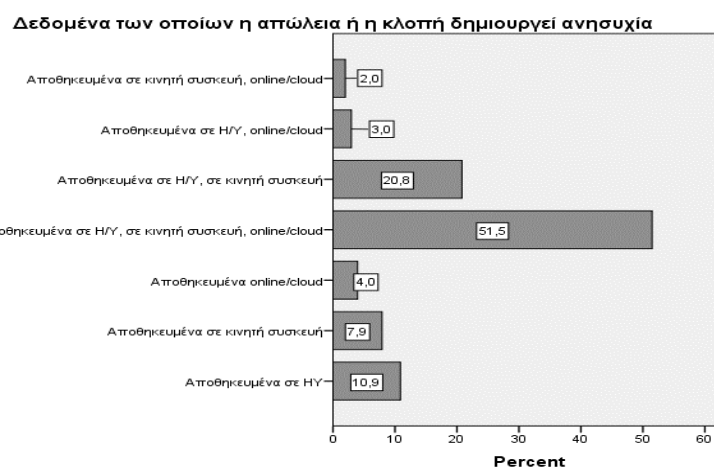
N	Valid	101
	Missing	0
Mean		15,3762
Median		16,0000
Mode		15,00 ^a
Minimum		6,00
Maximum		20,00

a. Multiple modes exist. The smallest value is shown

Πίνακας 5. Μ.Ο ανησυχιών υποκειμένων δεδομένων

Στην ερώτηση Γ.1.8, οι συμμετέχοντες κλήθηκαν να απαντήσουν αν θα ήθελαν να έχουν πληροφόρηση στην περίπτωση που χαθούν ή κλαπούν τα προσωπικά τους δεδομένα. Από τους 101 ερωτηθέντες, 99 απάντησαν θετικά, ένας/μια αρνητικά και ένας/μια δεν απάντησε. Η ανάγκη ενημέρωσης σε περίπτωση απώλειας ή κλοπής προσωπικών δεδομένων καταδεικνύεται εμφατικά και στην έρευνα του 2015 (European Commission/Eurobarometer 2015), όπου το 97% των Ελλήνων συμμετεχόντων απάντησε θετικά και 3% αρνητικά.

Στο ερώτημα ποιων δεδομένων η κλοπή ή η απώλεια θα ανησυχούσε περισσότερο τους ερωτώμενους εστίασε η ερώτηση Γ.1.9. Τα αποτελέσματα της έρευνας (Διάγραμμα 21) δείχνουν ότι πάνω από τους μισούς των ερωτηθέντων (51.5%) δηλώνουν ότι ανησυχούν εξίσου για την απώλεια δεδομένων αποθηκευμένων στον Η/Υ, τις κινητές συσκευές και online/cloud. Εξετάζοντας τις απαντήσεις μεμονωμένα διαπιστώνεται ότι η ανησυχία για δεδομένα αποθηκευμένα στον Η/Υ φτάνει το 86,2%, σε κινητές συσκευές 82,2% και online/cloud 58,5%.



Διάγραμμα 21. Δεδομένα των οποίων η απώλεια ή η κλοπή δημιουργεί ανησυχία

Στην ίδια ερώτηση, η έρευνα του 2015 (European Commission/Eurobarometer 2015) έδειξε υψηλότερα ποσοστά, σε επίπεδο Μ.Ο Ευρώπης για δεδομένα αποθηκευμένα σε Η/Υ (56%) και σε κινητές συσκευές (52%), ενώ χαμηλότερα για δεδομένα αποθηκευμένα online ή στο cloud (30%). Ωστόσο, με αναφορά στην Ελλάδα καταγράφηκε ισχυρότερη ανησυχία για τα δεδομένα σε κινητές συσκευές (64%) σε σχέση με την Ευρώπη. Ανησυχία για δεδομένα αποθηκευμένα σε Η/Υ ή αποθηκευμένα online ή στο cloud καταδείχθηκε σε ποσοστό 50% και 35% αντίστοιχα.

Στην τελευταία ερώτηση (Γ.1.10) της υποενότητας Γ.1 επιχειρήθηκε η διερεύνηση της φύσης του κινδύνου που οι ερωτώμενοι βιώνουν όταν παρέχουν προσωπικές πληροφορίες online. Τα αποτελέσματα των απαντήσεων των ερωτώμενων (Πίνακας 6) καταγράφονται συγκριτικά με τα αντίστοιχα στην ίδια ερώτηση της πανευρωπαϊκής έρευνας του 2015 (European Commission/Eurobarometer 2015).

	Παρούσα έρευνα	Ελλάδα (2015)	Ευρώπη (Μ.Ο) (2015)
<i>Να πέσετε θύμα απάτης</i>	76.2%	50%	50%
<i>Η ψηφιακή σας ταυτότητα να χρησιμοποιηθεί για λόγους απάτης</i>	77.2%	31%	40%
<i>Οι πληροφορίες σας να χρησιμοποιηθούν χωρίς να το γνωρίζετε</i>	63.4%	39%	32%
<i>Να κλαπούν οι προσωπικές σας πληροφορίες</i>	65.3%	33%	29%

Οι πληροφορίες σας να διανεμηθούν σε τρίτους (εταιρίες ή κρατικές υπηρεσίες) χωρίς τη συγκατάθεσή σας	64.4%	21%	25%
Οι πληροφορίες σας να χρησιμοποιηθούν σε διαφορετικό πλαίσιο για διαφορετικό λόγο από αυτόν που τις παρέχετε αρχικά	57.4%	24%	20%
Οι πληροφορίες σας να χρησιμοποιηθούν για να σας αποσταλεί ανεπιθύμητο διαφημιστικό υλικό	34.7%	10%	19%
Η προσωπική σας ασφάλεια να τεθεί σε κίνδυνο	74.3%	26%	18%
Να πληγεί η φήμη σας	55.4%	6%	7%
Να πέσετε θύμα διακρίσεων (πχ προσλήψεις εργασίας, να σας χρεώσουν υψηλότερες τιμές, να σας απαγορευθεί η πρόσβαση σε κάποια υπηρεσία)	47.5%	4%	5%
Οι απόψεις σας και η συμπεριφορά σας να παρεξηγηθούν	37.6%	9%	5%

Πίνακας 6. Κίνδυνοι για τα προσωπικά δεδομένα

Τα ευρήματα της έρευνας δείχνουν ότι οι ερωτώμενοι ανησυχούν περισσότερο για ζητήματα ασφάλειας και χρήσης των προσωπικών τους δεδομένων για λόγους απάτης, ενώ έπονται οι ανησυχίες για την χρησιμοποίηση των πληροφοριών τους χωρίς να το γνωρίζουν ή τη διανομή τους σε τρίτους χωρίς τη συγκατάθεσή τους. Η ανησυχία για την παρερμηνεία των απόψεων και της συμπεριφοράς τους, όπως και η ανησυχία για την αποστολή ανεπιθύμητου διαφημιστικού υλικού καταγράφονται σε μικρότερα ποσοστά.

5.4. Ενότητα Γ, υποενότητα Γ.2 «Προστασία Προσωπικών Δεδομένων»

Η συγκεκριμένη υποενότητα Γ.2 με 7 ερωτήσεις διερευνά τις πρακτικές των συμμετεχόντων σε σχέση με την προστασία των προσωπικών τους δεδομένων.

Η ενημέρωση για τη συλλογή και την επεξεργασία των προσωπικών δεδομένων είναι προαπαιτούμενο για τον έλεγχο των δεδομένων από τα υποκείμενα αυτών, ώστε να πάρουν τεκμηριωμένες αποφάσεις για την προστασία τους. Οι πάροχοι μπορούν να παράσχουν την ενημέρωση αυτή με τις πολιτικές απορρήτου, αλλά τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν πρόβλημα στην κατανόηση της ενημέρωσης. Η

βιβλιογραφία έχει δείξει ότι συχνά τα υποκείμενα των δεδομένων δεν διαβάζουν τις πολιτικές απορρήτου και αυτό αποτελεί μια επικίνδυνη συμπεριφορά (Marwick, Murgia-Diaz, & Palfrey 2010). Στην ερώτηση Γ.2.1, οι συμμετέχοντες κλήθηκαν να απαντήσουν αν διαβάζουν τις πολιτικές απορρήτου ολόκληρες, μερικώς ή δεν τις διαβάζουν. Μόνο 6.9% διαβάζει όλο το κείμενο, 28.7% δεν τις διαβάζει και 64.4% τις διαβάζει μερικώς. Υψηλότερο ποσοστό (37%) όσων διαβάζουν ολόκληρο το κείμενο της πολιτικής απορρήτου έδειξε η έρευνα του 2015 (European Commission/Eurobarometer 2015) για την Ελλάδα. Το ποσοστό των ερωτώμενων που τις διάβαζε μερικώς ήταν 35%, ενώ εκείνο όσων δεν τις διάβαζαν 27%.

Αναγνωρίζοντας την τάση οι χρήστες να διαβάζουν μερικώς ή να μην διαβάζουν τις πολιτικές απορρήτου, η ερώτηση Γ.2.2 επιχείρησε να διερευνήσει τους λόγους. Θα πρέπει να σημειωθεί στο σημείο αυτό ότι 6 από τους 7 ερωτώμενους που στην προηγούμενη ερώτηση είχαν απαντήσει ότι διαβάζουν ολόκληρο το κείμενο, παρείχαν λόγους για μερική ή καθόλου ανάγνωση. Τα αποτελέσματα των απαντήσεων που καταγράφουν τους λόγους για την μερική ή καθόλου ανάγνωση των πολιτικών απορρήτου παρουσιάζονται συγκριτικά με την έρευνα του 2015 (European Commission/Eurobarometer 2015) στον ακόλουθο Πίνακα 7, καταδεικνύοντας υψηλά ποσοστά απαντήσεων με αναφορά στην έκταση του κειμένου (73.4%) και στο γεγονός ότι ο τρόπος γραφής τους είναι δυσνόητος (55.4%).

Μελέτες έχουν δείξει ότι όταν οι πολιτικές απορρήτου είναι δύσκολα αναγνώσιμες (Cadogan 2001, Proctor, Athar Ali & Vu 2008) σπάνια να τις διαβάζουν οι χρήστες. Το χαμηλό ποσοστό ανάγνωσης οφείλεται κυρίως στην πολυπλοκότητα των πολιτικών απορρήτου, τη χρήση τεχνικών όρων και την ιδιαίτερα μεγάλη έκτασή τους. Αντιθέτως, όταν οι πολιτικές απορρήτου διαβάζονται εύκολα, αυξάνεται η εμπιστοσύνη των χρηστών στους παρόχους υπηρεσιών (Bansal & Zahedi 2008, Milne & Culnan 2004). Όπως σημειώνουν οι van Ooijen & Vrabec (2019) όταν οι πολιτικές αλλάζουν, τα υποκείμενα των δεδομένων πρέπει να τις διαβάσουν εκ νέου για να κατανοήσουν για τις επιπτώσεις για τα προσωπικά τους δεδομένα.

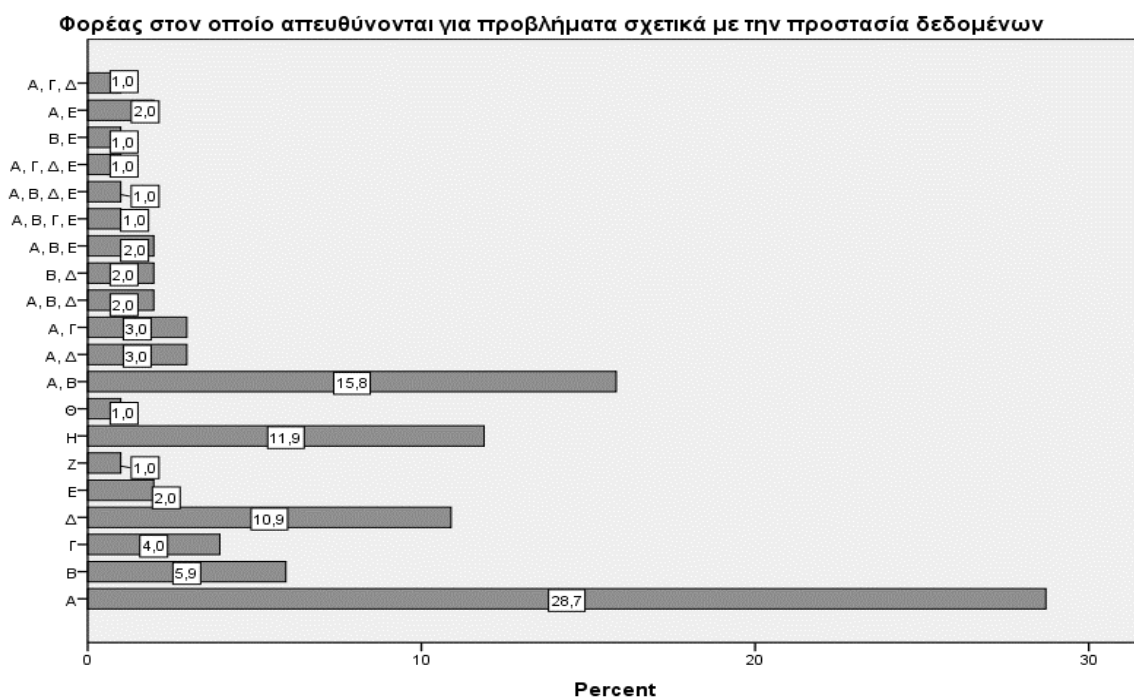
	Παρούσα έρευνα	Ελλάδα (2015)	Ευρώπη (Μ.Ο) (2015)
<i>Είναι πολύ μεγάλο το κείμενο για να το διαβάσω</i>	74.3%	55%	67%
<i>Δεν είναι ξεκάθαρες, είναι δυσνόητες</i>	55.4%	28%	38%
<i>Πιστεύετε ότι οι ιστότοποι δεν θα τις τηρήσουν έτσι και αλλιώς</i>	21.8%	19%	15%
<i>Πιστεύετε ότι η νομοθεσία θα σας προστατεύσει σε κάθε περίπτωση</i>	8.9%	9%	14%
<i>Σας αρκεί να βλέπετε ότι οι ιστότοποι διαθέτουν πολιτικές απορρήτου</i>	13.9%	21%	14%
<i>Δεν νομίζετε ότι είναι κάτι σημαντικό για να τις διαβάσετε</i>	4%	19%	9%
<i>Δεν γνωρίζετε που να τις βρείτε</i>	2%	11%	7%
<i>Άλλο</i>	3%	4%	5%

Πίνακας 7. Λόγοι μη ανάγνωσης ή μερικής ανάγνωσης των πολιτικών απορρήτου

Ποσοστό 21.8% των συμμετεχόντων δήλωσε ως λόγο μη ανάγνωσης ή μερικής ανάγνωσης των πολιτικών απορρήτου ότι «οι ιστότοποι δεν θα τις τηρήσουν έτσι και αλλιώς», γεγονός που δείχνει την απουσία εμπιστοσύνης στους παρόχους. Από την άλλη πλευρά, 13.9% των ερωτώμενων δήλωσε ότι αρκείται να βλέπει ότι υπάρχει πολιτική απορρήτου, γεγονός που υποδηλώνει την εμπιστοσύνη τους στους παρόχους. Οι Hoofnagle & Urban (2014) στην έρευνα τους έδειξαν ότι 62% των συμμετεχόντων θεωρούσε ότι η ύπαρξη πολιτικής απορρήτου σε έναν ιστότοπο δεν θα επέτρεπε το διαμοιρασμό προσωπικών πληροφοριών τους χωρίς την άδειά τους. Είναι προφανές ότι μια τέτοια θεώρηση μειώνει τις ανησυχίες ιδιωτικότητας και αυξάνει τη συμπεριφορά αποκάλυψης πληροφοριών.

Στους συμμετέχοντες τέθηκε το ερώτημα (Γ.2.3) «Σε ποιόν θα απευθυνθείτε σε περίπτωση που αντιμετωπίζετε κάποιο πρόβλημα σχετικά με την προστασία των προσωπικών σας δεδομένων;» με δυνατότητα πολλαπλών επιλογών. Η γνώση του φορέα στον οποίο πρέπει να απευθυνθούν τα υποκείμενα των δεδομένων σε περίπτωση προβλήματος είναι ένδειξη της κατανόησης του δικαιώματός τους σε ένδικα μέσα. Τα αποτελέσματα των απαντήσεων δείχνουν ότι 11.9% των ερωτώμενων δεν γνωρίζουν

πού πρέπει να απευθυνθούν και 1% ότι δεν θα απευθυνθεί σε κανέναν. Με ποσοστό 28.7% εμφανίζεται η επιλογή «Αρμόδια Ρυθμιστική Αρχή» και με ποσοστό 10.9% η επιλογή «Κάποια Ανεξάρτητη Αρχή για την προστασία του υποκειμένου των δεδομένων». Σε χαμηλότερα ποσοστά, οι ερωτώμενοι επέλεξαν «Αρχή ή ιδιωτικός φορέας που διαχειρίζεται τα δεδομένα σας», «Δικαστήριο» και «Ευρωπαϊκή Αρχή» (5.9%, 4% και 2% αντίστοιχα), ενώ εμφανίζεται και συνδυασμός επιλογών, όπως καταγράφεται στο ακόλουθο Διάγραμμα 22.



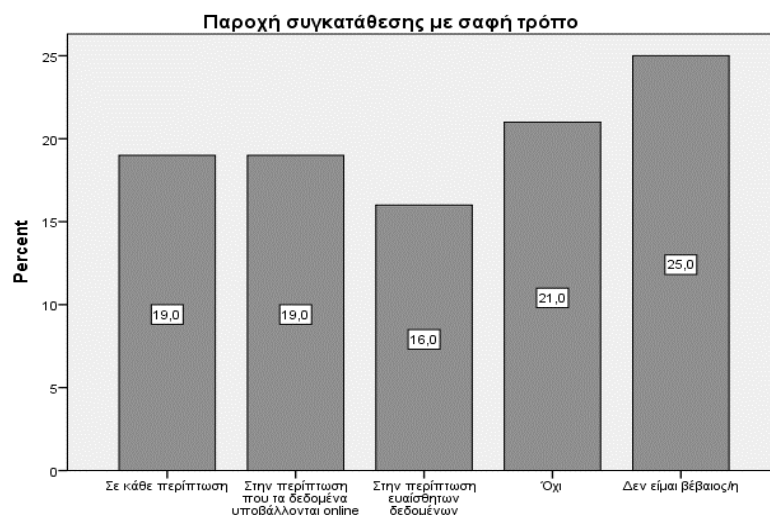
Α. Αρμόδια Ρυθμιστική Αρχή Β. Αρχή ή ιδιωτικός φορέας που διαχειρίζεται τα δεδομένα σας Γ. Δικαστήριο Δ. Κάποια Ανεξάρτητη Αρχή για την προστασία του υποκειμένου των δεδομένων Ε. Ευρωπαϊκή Αρχή Ζ. Άλλο Η. Δεν γνωρίζω Θ. Δεν θα απευθυνθώ σε κανέναν

Διάγραμμα 22. Φορέας στον οποίο απευθύνονται τα υποκείμενα των δεδομένων για την άσκηση ένδικων μέσων

Τα αποτελέσματα της έρευνας του 2015 (European Commission/Eurobarometer 2015) έδειξαν ότι οι Έλληνες ερωτώμενοι προέκριναν την Αρμόδια Εθνική Ρυθμιστική Αρχή (63%), Αρχή ή ιδιωτικό φορέα που διαχειρίζεται τα δεδομένα (47%), Δικαστήριο (22%), κάποια Ανεξάρτητη Αρχή για την Προστασία των δεδομένων (15%), Ευρωπαϊκή Αρχή (4%). Τα αντίστοιχα ποσοστά σε επίπεδο Μ.Ο Ευρώπης ήταν 50%, 45%, 21%, 12%, 4%. Το ποσοστό όσων δεν γνώριζαν πού να απευθυνθούν ήταν 8% Μ.Ο. Ευρώπης και 3% Ελλάδα.

Στη βάση της προβλεπόμενης από τον ΓΚΠΔ απαίτησης για ελεύθερη και ρητή συγκατάθεση, προκειμένου για την χρήση των δεδομένων του υποκειμένου, συντάχθηκε

η ερώτηση Γ.2.4 «Δίνετε με σαφή τρόπο τη συγκατάθεση σας προκειμένου κάθε είδος προσωπικής πληροφορίας να συλλεγεί και να επεξεργαστεί;». Όπως προκύπτει από το Διάγραμμα 23, το 1/4 των ερωτώμενων (25%) δεν είναι βέβαιοι ότι παρέχουν με ρητό τρόπο τη συγκατάθεσή τους και 21% δεν το κάνει. Από τους υπόλοιπους, 19% δηλώνει ότι το κάνει σε κάθε περίπτωση, ίδιο ποσοστό στην περίπτωση που τα δεδομένα ζητούνται online και 16% μόνο στην περίπτωση ευαίσθητων δεδομένων.

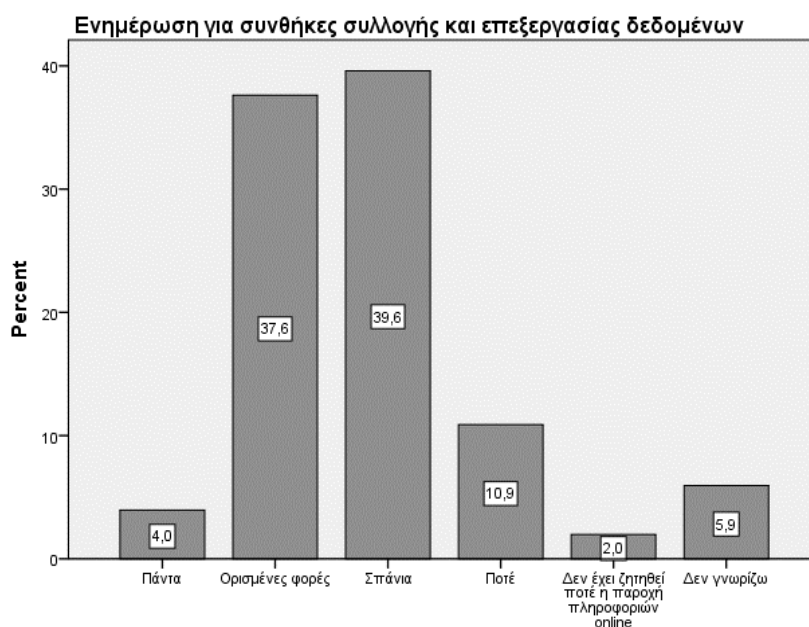


Διάγραμμα 23. Παροχή ρητής συγκατάθεσης των υποκειμένων των δεδομένων

Στην έρευνα του 2015 (European Commission/Eurobarometer 2015) είχε συμπεριληφθεί ερώτηση αν θα πρέπει να δίνεται ρητά η συγκατάθεση του υποκειμένου για τη συλλογή και επεξεργασία δεδομένων του. Τα αποτελέσματα της έρευνας έδειξαν ως ισχυρότερη απάντηση «σε όλες τις περιπτώσεις» (69% Μ.Ο. Ευρώπης, 77% Ελλάδα), ακολουθούμενη από την απάντηση «στην περίπτωση που τα δεδομένα ζητούνται online» (14% Μ.Ο. Ευρώπης, 11% Ελλάδα). Θετική απάντηση για τα ευαίσθητα δεδομένα μόνο δόθηκε από 10% των ερωτώμενων στην Ευρώπη (Μ.Ο) και 11% των Ελλήνων, ενώ η απάντηση «όχι» (5% Μ.Ο. Ευρώπης, 1% Ελλάδα), και «δεν είμαι βέβαιος» (4% Μ.Ο. Ευρώπης, 2% Ελλάδα), επελέγησαν σε χαμηλότερα ποσοστά.

Οι χρήστες πρέπει να γνωρίζουν τον τρόπο που μια εταιρεία σκοπεύει να χρησιμοποιήσει τα προσωπικά τους δεδομένα και να δίνουν τη συγκατάθεσή τους για την χρήση ή να έχουν το δικαίωμα να μην συμμετέχουν, εφόσον η συγκατάθεση αποτελεί τη βάση της επεξεργασίας των δεδομένων. Οι όροι και οι προϋποθέσεις δεν πρέπει να προκαλούν σύγχυση ή να διατρέχουν πολλές νομικού περιεχομένου σελίδες και η όλη διαδικασία πρέπει να χαρακτηρίζεται από διαφάνεια και σαφήνεια (Datoo 2018). Η ερώτηση Γ.2.5,

λοιπόν, εστιάζει στην ενημέρωση που έχουν τα υποκείμενα των δεδομένων για τις συνθήκες συλλογής και επεξεργασίας των δεδομένων τους, όταν παρέχονται προσωπικές πληροφορίες online. Τα αποτελέσματα από τις απαντήσεις (Διάγραμμα 24) δείχνουν ότι 5.9% δεν γνωρίζει, μόνο 4% των ερωτώμενων απάντησαν «πάντα» και 10.9% «ποτέ», ενώ υψηλά ποσοστά καταγράφηκαν για «ορισμένες φορές» (37.6%) και «σπάνια» (39.6%)

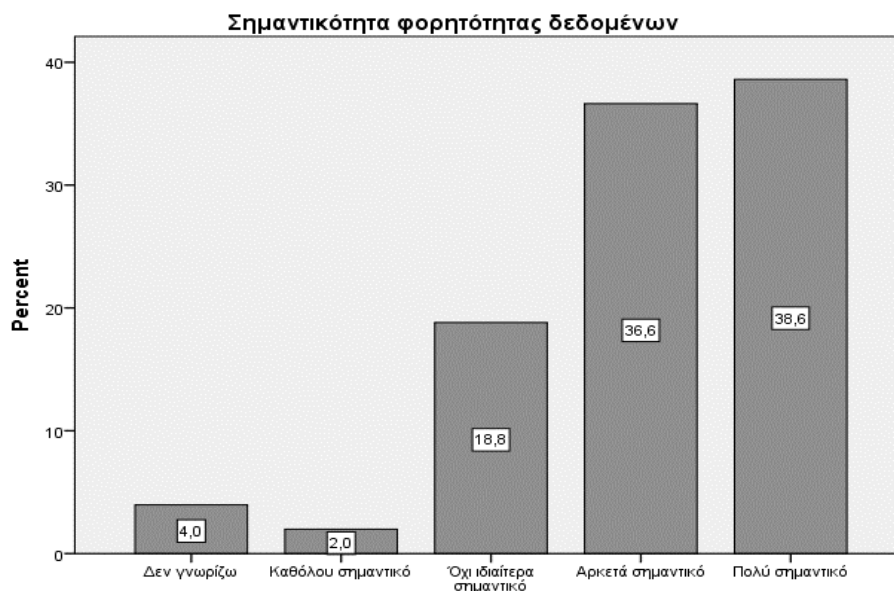


Διάγραμμα 24. Ενημέρωση των υποκειμένων των δεδομένων για συνθήκες συλλογής και επεξεργασίας των δεδομένων τους

Τα αποτελέσματα της έρευνας του 2015 (European Commission/Eurobarometer 2015) έδειξαν ως επικρατέστερη απάντηση «μερικές φορές» (41% Μ.Ο. Ευρώπης, 37% στην Ελλάδα). Με αναφορά στην Ελλάδα, το ποσοστό απαντήσεων «πάντα» υπερέβαινε το «σπάνια» (29% και 18% αντίστοιχα), ενώ μόνο 9% των ερωτώμενων δήλωσε «ποτέ».

Το δικαίωμα της φορητότητας ουσιαστικά συνίσταται στο δικαίωμα του υποκειμένου να έχει πρόσβαση στα δεδομένα του που έτυχαν επεξεργασίας -αυτό επιτρέπει στο υποκείμενο να αναγνωρίσει και αν η επεξεργασία ήταν σύννομη- και στο δικαίωμα να μεταφέρει τα δεδομένα σε άλλο πάροχο, χωρίς εμπόδια (van Ooijen & Vrabec 2019). Η ερώτηση Γ.2.6 εστιάζει στη σπουδαιότητα του δικαιώματος στη φορητότητα. Όπως καταγράφεται στο Διάγραμμα 25, η πλειονότητα των ερωτώμενων θεωρεί πολύ σημαντική (38.6%) ή αρκετά σημαντική (36.6%) τη δυνατότητα της φορητότητας, παρά το γεγονός ότι σε ερώτηση προηγούμενης ενότητας (B.12) το ποσοστό όσων δεν είχαν ή είχαν μικρή γνώση του σχετικού δικαιώματος ήταν 54%. Δεν θεωρείται καθόλου

σημαντική η δυνατότητα της φορητότητας από 2% των ερωτώμενων, ενώ 18.8% την θεωρεί όχι ιδιαίτερα σημαντική. Τέλος, 4% δήλωσε «δεν γνωρίζω». Η αποτυχία των χρηστών να αναγνωρίσουν τη σημασία της φορητότητας των δεδομένων είναι κρίσιμη για την αποτελεσματική εφαρμογή του ΓΚΠΔ (Sobolewski, Mazur, & Paliński 2017).



Διάγραμμα 25. Άποψη των υποκειμένων των δεδομένων για τη σημασία της φορητότητας των δεδομένων

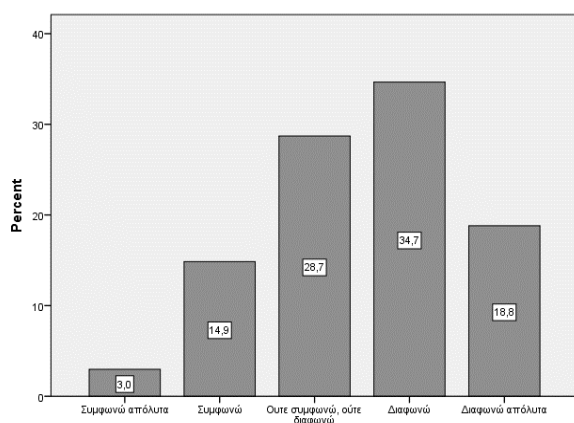
Το δικαίωμα στη φορητότητα των δεδομένων αποτελεί ουσιαστικό στοιχείο στην ενδυνάμωση του δικαιώματος ελέγχου που έχουν τα υποκείμενα των δεδομένων και ένα πρώτο βήμα στην κατεύθυνση της «προεπιλεγμένης κυριότητας» των προσωπικών δεδομένων από τα υποκείμενα που αυτά αφορούν (De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez 2018: 201). Ωστόσο, το δικαίωμα στη φορητότητα δεν ισχύει για όλα τα προσωπικά δεδομένα, παρά μόνο γι' αυτά που έχει παράσχει το ίδιο το υποκείμενο. Επιπλέον, η μεταφορά των δεδομένων δεν σημαίνει αυτόματα και διαγραφή τους από τον αρχικό πάροχο. Για να συμβεί αυτό απαιτείται αίτημα διαγραφής (van Ooijen & Vrabec 2019).

Η τελευταία ερώτηση (Γ.2.7) περιέχει 6 φράσεις, στις οποίες οι ερωτώμενοι κλήθηκαν να δηλώσουν τη συμφωνία/τη διαφωνία τους :

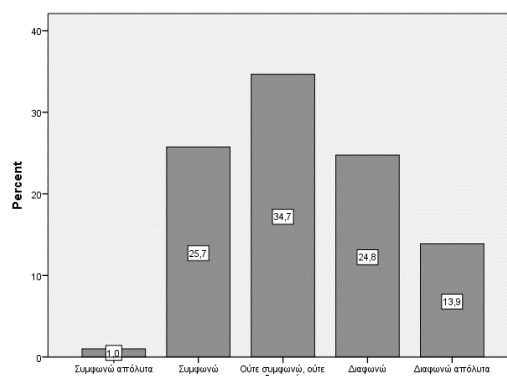
- α) Είμαι βέβαιος/η ότι τα προσωπικά δεδομένα που παρέχω δεν αξιοποιηθούν από κανέναν άλλο,
- β) Γνωρίζω καλά τη νομοθεσία για την προστασία των δεδομένων μου για να προστατεύσω τον εαυτό μου,

- γ) Εμπιστεύομαι τους παρόχους υπηρεσιών για να προστατεύουν τα δεδομένα μου,
- δ) Η νομοθεσία και οι ρυθμιστικές αρχές προστατεύουν πλήρως τα προσωπικά μου δεδομένα,
- ε) Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online
- στ) Οι κυβερνήσεις προστατεύουν τα δεδομένα μου.

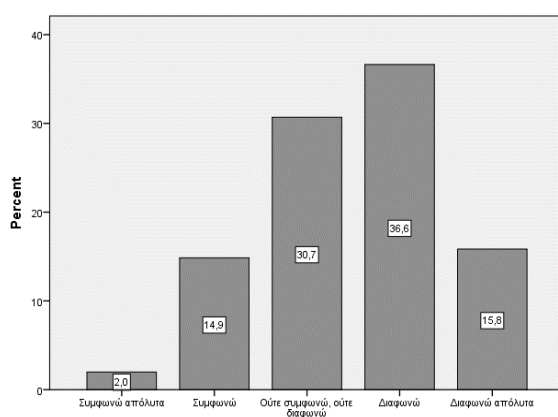
Τα αποτελέσματα εμφανίζονται στα Διαγράμματα 26-31 που ακολουθούν.



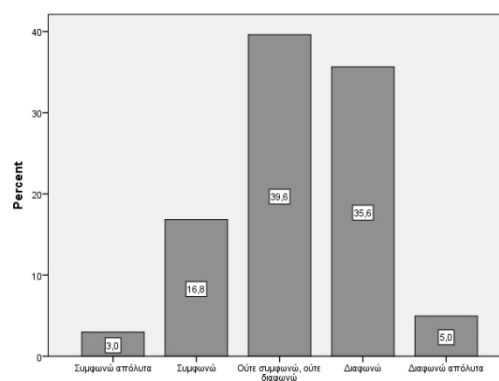
Διάγραμμα 26. Άποψη ερωτώμενων για τη δήλωση «Είμαι βέβαιος/η ότι τα προσωπικά δεδομένα που παρέχω δεν αξιοποιηθούν από κανέναν άλλο»



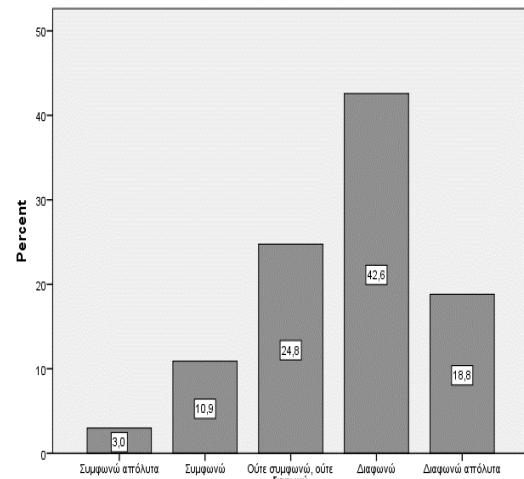
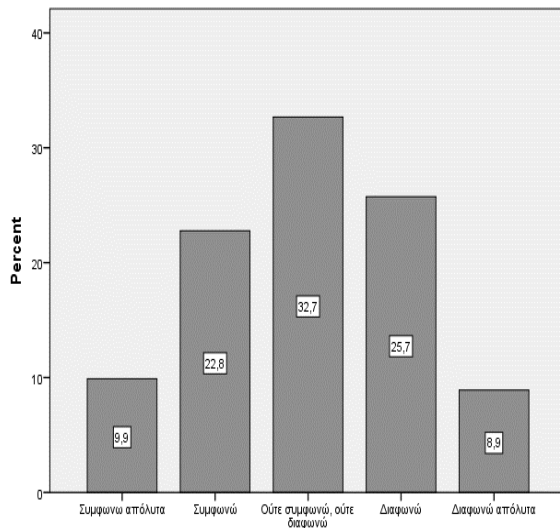
Διάγραμμα 27. Άποψη ερωτώμενων για τη δήλωση «Γνωρίζω καλά τη νομοθεσία για την προστασία των δεδομένων μου για να προστατεύσω τον εαυτό μου»



Διάγραμμα 28. Άποψη ερωτώμενων για τη δήλωση «Εμπιστεύομαι τους παρόχους υπηρεσιών για να προστατεύουν τα δεδομένα μου»



Διάγραμμα 29. Άποψη ερωτώμενων για τη δήλωση «Η νομοθεσία και οι ρυθμιστικές αρχές προστατεύουν πλήρως τα προσωπικά μου δεδομένα»



Διάγραμμα 30. Αποψη ερωτώμενων για τη δήλωση «Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online»

Διάγραμμα 31. Άποψη ερωτώμενων για τη δήλωση «Οι κυβερνήσεις προστατεύουν τα δεδομένα μου»

Τα αποτελέσματα αυτά συγκρίνονται στο Πίνακα 8.

	Συμφωνώ απόλυτα	Συμφωνώ	Ούτε συμφωνώ, ούτε διαφωνώ	Διαφωνώ	Διαφωνώ απόλυτα
Είμαι βέβαιος ότι τα προσωπικά δεδομένα...	3%	14.9%	28.7%	34.7%	18.8%
	17.90%			53.50%	
Γνωρίζω καλά τη νομοθεσία...	1%	25.7%	34.7%	24.8%	13.9%
	26.70%			38.70%	
Εμπιστεύομαι τους παρόχους....	2%	14.9%	30.7%	36.6%	15.8%
	16.90%			52.40%	
Η νομοθεσία και οι ρυθμιστικές αρχές.....	3%	16.8%	39.6%	35.6%	5%
	19.80%			40.60%	
Για να προστατευθώ είναι αρκετό...	9.9%	22.8%	32.7%	25.7%	8.9%
	32.70%			34.60%	
Οι κυβερνήσεις προστατεύουν τα δεδομένα μου...	3%	10.9%	24.8%	42.6%	18.8%
	13.90%			61.40%	

Πίνακας 8. Αποτελέσματα απαντήσεων σε ερώτηση Γ.2.7

Σε καμία από τις 6 δηλώσεις δεν καταγράφηκαν ποσοστά συμφωνίας ή απόλυτης συμφωνίας υψηλότερα από τα ποσοστά διαφωνίας ή απόλυτης διαφωνίας. Σε 5 από τις 6 δηλώσεις, τα ποσοστά συμφωνίας ή απόλυτης συμφωνίας ήταν επίσης χαμηλότερα

από τα ποσοστά της απάντησης «ούτε συμφωνώ, ούτε διαφωνώ». Εξάιρεση αποτελεί η δήλωση «Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online». Τα υψηλότερα ποσοστά διαφωνίας ή απόλυτης διαφωνίας καταγράφηκαν στις δηλώσεις «Οι κυβερνήσεις προστατεύουν τα δεδομένα μου» (61.4%), «Είμαι βέβαιος/η ότι τα προσωπικά δεδομένα που παρέχω δεν αξιοποιηθούν από κανέναν άλλο» (53.5%) και «Εμπιστεύομαι τους παρόχους υπηρεσιών για να προστατεύουν τα δεδομένα μου» (52.4%). Στην περίπτωση της δήλωσης «Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online», το ποσοστό της διαφωνίας ή απόλυτης διαφωνίας είναι ελάχιστα μεγαλύτερο από το αντίστοιχο της απόλυτης συμφωνίας ή συμφωνίας και της απάντησης «ούτε συμφωνώ, ούτε διαφωνώ».

Αν και τα αποτελέσματα της έρευνας δεν έδειξαν υψηλό βαθμό γνώσης των υποκειμένων των δεδομένων για τα δικαιώματά τους που είχε τεθεί ως όρος της ερευνητικής υπόθεσης (*Ο υψηλός βαθμός γνώσης των δικαιωμάτων των υποκειμένων, όπως καταγράφονται στον ΓΚΠΔ, αυξάνει τις ανησυχίες ιδιωτικότητας και επιδρά θετικά στη συμπεριφορά προστασίας προσωπικών δεδομένων*), επιχειρείται, ωστόσο, η διερεύνηση δύο συσχετισμών.

A) Σχετίζονται οι ανησυχίες που μελετήθηκαν (Γ.1.3-Γ.1.7) με τη συμφωνία ή τη διαφωνία των υποκειμένων των δεδομένων με τις δηλώσεις της ερώτησης Γ.2.7;

B) Σχετίζεται ο βαθμός γνώσης των δικαιωμάτων των υποκειμένων (B.1-B.12) με τις δηλώσεις της ερώτησης Γ.2.7.

Για να εξεταστεί η πρώτη συσχέτιση, μετά τη διατύπωση της μηδενικής και της εναλλακτικής υπόθεσης (H_0 : Οι ανησυχίες των υποκειμένων των δεδομένων δεν συσχετίζονται με τις δηλώσεις τους. H_1 : Οι ανησυχίες των υποκειμένων των δεδομένων συσχετίζονται με τις δηλώσεις τους), χρησιμοποιήθηκε ο συντελεστής Pearson r .

Τα αποτελέσματα εμφανίζονται στον ακόλουθο πίνακα 9:

		Total_score_worries	Total_score_statements
Total_score_worries	Pearson Correlation	1	,220*
	Sig. (2-tailed)		,027
	N	101	101
Total_score_statements	Pearson Correlation	,220*	1
	Sig. (2-tailed)	,027	
	N	101	101

*. Correlation is significant at the 0.05 level (2-tailed).

Πίνακας 9. Πίνακας συσχέτισης ανησυχιών με δηλώσεις υποκειμένων δεδομένων

Το αποτέλεσμα της συσχέτισης είναι στατιστικά σημαντικό σε επίπεδο σημαντικότητας $p < 0,05$. Ωστόσο η τιμή του δείκτη συσχέτισης είναι πολύ χαμηλή ($r = 0,22$), γεγονός που σύμφωνα με τους βαθμούς του συντελεστή συσχέτισης (Ρούσσοσ & Τσαούσης 2011) δεν επιτρέπει να θεωρήσουμε ότι οι ανησυχίες των υποκειμένων των δεδομένων σχετίζονται επαρκώς με τις απαντήσεις τους στις δηλώσεις της ερώτησης Γ.2.7.

Ο δεύτερος συσχετισμός ελέγχθηκε, επίσης, με τη χρήση συντελεστή Pearson r και τα αποτελέσματα παρουσιάζονται στον πίνακα 10.

		Total_score_statements	Total_score_rights
Total_score_statements	Pearson Correlation	1	-,489**
	Sig. (2-tailed)		,000
	N	101	101
Total_score_rights	Pearson Correlation	-,489**	1
	Sig. (2-tailed)	,000	
	N	101	101

** . Correlation is significant at the 0.01 level (2-tailed).

Πίνακας 10. Πίνακας συσχέτισης βαθμού γνώσης δικαιωμάτων με δηλώσεις υποκειμένων δεδομένων

Καθώς το αποτέλεσμα της συσχέτισης είναι στατιστικά σημαντικό σε επίπεδο σημαντικότητας $p < 0,01$, η μηδενική υπόθεση (H_0) που πρότεινε ότι δεν υπάρχει συσχέτιση μεταξύ του βαθμού γνώσης δικαιωμάτων και των δηλώσεων των

υποκειμένων των δεδομένων πρέπει να απορριφθεί. Η τιμή του δείκτη συσχέτισης είναι ωστόσο χαμηλή ($r=-0,48$), σύμφωνα με τους βαθμούς του συντελεστή συσχέτισης (Ρούσος & Τσαούσης 2011). Αυτό μας επιτρέπει να θεωρήσουμε ότι υπάρχει χαμηλή συσχέτιση μεταξύ των δύο μεταβλητών και μάλιστα καθώς αυξάνεται η μία, μειώνεται η άλλη (αρνητικό πρόσημο του συντελεστή). Άρα όσο θα αυξάνεται η γνώση των υποκειμένων των δεδομένων για τα δικαιώματά τους θα μειώνεται η συμφωνία τους με τις προτεινόμενες δηλώσεις.

Τα αποτελέσματα της έρευνας παρουσιάζουν ενδιαφέρον, καθώς δείχνουν ότι ένα χρόνο μετά την εφαρμογή του ΓΚΠΔ, οι χρήστες δεν έχουν υψηλό βαθμό γνώσης όλων των δικαιωμάτων για τα οποία ερωτήθηκαν, ενώ σε αρκετές περιπτώσεις δεν γνωρίζουν και υπό ποιες προϋποθέσεις μπορούν να ασκήσουν αυτά. Ενδιαφέρον παρουσιάζει το γεγονός ότι διέκριναν μεταξύ του ελέγχου που έχουν ως χρήστες στο στάδιο της ανάρτησης και του ελέγχου μετά από αυτήν (πρόσβαση, χρήση κ.λπ). Όπως αναμενόταν, τα υποκείμενα των δεδομένων ανησυχούν για το ποιος και πώς διαχειρίζεται τα δεδομένα τους και για τους κινδύνους από την κλοπή ή την απώλεια αυτών. Ωστόσο, όπως καταγράφεται στα αποτελέσματα της έρευνας, οι περισσότεροι διαβάζουν μερικώς τις πολιτικές απορρήτου, 1/4 των ερωτώμενων δεν είναι βέβαιοι ότι παρέχουν με ρητό τρόπο τη συγκατάθεσή τους και πολλοί δήλωσαν ότι σπάνια ή ορισμένες φορές έχουν ενημέρωση για τη συλλογή και επεξεργασία των δεδομένων τους που είναι προϋπόθεση για την παροχή της συγκατάθεσής τους.

Κεφάλαιο 6

Συμπεράσματα

Αν και σημαντικά βήματα έχουν γίνει σε ευρωπαϊκό επίπεδο για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων ήδη από την εφαρμογή της Οδηγίας 95/46 ΕΕ, σημαντικές αποκλίσεις έχουν διαπιστωθεί, μεταξύ των κρατών-μελών, σε επίπεδο νομοθεσίας και εφαρμογής της. Ταυτόχρονα, ο ρόλος και η αλληλεπίδραση μεταξύ κυβερνήσεων, οργανώσεων προστασίας δικαιωμάτων και Αρχών Προστασίας Δεδομένων διαφέρουν από χώρα σε χώρα. Διαφορές εντοπίζονται και στην ένταση και το εύρος, των ενημερωτικών εκστρατειών, της προσοχής των μέσων ενημέρωσης και του δημόσιου διαλόγου όσον αφορά την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Έτσι, σε ορισμένες χώρες γίνεται συζήτηση γύρω από έννοιες όπως η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, η προστασία δεδομένων εξ ορισμού, οι ειδοποιήσεις παραβίασης δεδομένων και σε άλλες όχι (Custers, Dechesne, Sears, Tani & van der Hof 2018).

Στο πλαίσιο αυτό, ο πρόσφατα τεθείς σε εφαρμογή, σε επίπεδο Ευρωπαϊκής Ένωσης, Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) αναμένεται πως θα συμβάλλει θετικά, καθώς στοχεύει στην επίτευξη ισοδύναμου επιπέδου προστασίας διασφαλίζοντας «συνεκτική και ομοιόμορφη εφαρμογή των κανόνων για την προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση» (αιτιολογική σκέψη 10, 2016/679 ΕΕ).

Η ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων, ώστε να αυξηθεί ο έλεγχος που έχουν στα δεδομένα τους, είναι αναμφισβήτητη πρώτη προτεραιότητα του ΓΚΠΔ. Τα υποκείμενα των δεδομένων είναι καλύτερα ενημερωμένα, η συγκατάθεσή τους υπόκειται σε αυστηρότερους όρους, νέα δικαιώματα ενισχύουν τον έλεγχο των υποκειμένων στα δεδομένα τους όπως το δικαίωμα να ζητούν απάντηση από τον υπεύθυνο επεξεργασίας δεδομένων ή το δικαίωμα στη φορητότητα. Όπως σημειώνουν

οι van Ooijen & Vrabec (2019: 92) στον ΓΚΠΔ «η ανάγκη για έλεγχο από πλευράς των υποκειμένων φαίνεται να αντιμετωπίζεται πιο ρητά και με μεγαλύτερη προσοχή σε σύγκριση με τους παλαιότερους κανονισμούς».

Για να έχει όμως ουσιαστικό νόημα η ενίσχυση των δικαιωμάτων των υποκειμένων και να συμβάλλει αποτελεσματικά στην προστασία των δεδομένων τους, είναι μείζονος σημασίας η από πλευράς των υποκειμένων των δεδομένων γνώση των δικαιωμάτων τους ως προϋπόθεση για την άσκησή τους, παράλληλα με τις ατομικές στρατηγικές προστασίας της ιδιωτικότητας που εφαρμόζουν κατά την αλληλεπίδραση με άλλους και την παροχή πληροφοριών σε ψηφιακά περιβάλλοντα. Τόσο η γνώση σχετικά με τις τεχνικές και πρακτικές των οργανισμών και των παρόχων υπηρεσιών στη συλλογή και αξιοποίηση των δεδομένων των υποκειμένων, όσο και η γνώση για τη νομοθεσία και τις πολιτικές προστασίας βοηθούν τα υποκείμενα των δεδομένων να λάβουν τεκμηριωμένες αποφάσεις σε σχέση με την αποκάλυψη των προσωπικών τους δεδομένων και να ελέγξουν ή να βελτιστοποιήσουν την ιδιωτικότητά τους (Trepte et al. 2015, Park 2011).

Η παρούσα διπλωματική διατριβή, στο παραπάνω πλαίσιο, στόχευσε στη διερεύνηση της γνώσης ομάδας ενηλίκων χρηστών του Διαδικτύου και των ΜΚΔ για τα δικαιώματα που έχουν και τις νέες ρυθμίσεις στο θέμα της συλλογής και διαχείρισης προσωπικών τους δεδομένων από οργανισμούς, εταιρείες ή παρόχους. Συγκεκριμένα, με τη χρήση ερωτηματολογίου σε ομάδα ενηλίκων, εξετάστηκε ο βαθμός που τα υποκείμενα των δεδομένων που συμμετείχαν στην παρούσα διερευνητική έρευνα γνωρίζουν τη νέα νομοθεσία και κατανοούν τα δικαιώματα που θεσπίζονται γι' αυτά, ενώ επιχειρήθηκε και η ανίχνευση αντιλήψεών τους σε σχέση με τον έλεγχο της πληροφορίας, τις ανησυχίες ιδιωτικότητας και τη συμπεριφορά τους ως χρήστες.

Τα αποτελέσματα της έρευνας έδειξαν ότι μισοί σχεδόν από τους ερωτηθέντες είχαν πληροφόρηση για τον ΓΚΠΔ από το Διαδίκτυο (44.6%), ενώ περίπου 1/4 (24.8%) από προσωπική ενασχόληση/ενδιαφέρον, γεγονός που δείχνει ότι οι χρήστες ενδιαφέρονται για τη νομοθεσία προστασίας των δεδομένων τους. Αν και η συντριπτική πλειοψηφία αναγνώρισε ότι η εφαρμογή του ΓΚΠΔ αποτελεί ευθύνη σε επίπεδο Ευρωπαϊκής Ένωσης, σχεδόν 10% των ερωτηθέντων δεν γνώριζε ποιος έχει την ευθύνη εφαρμογής. Πληθώρα απαντήσεων καταγράφηκε στο ερώτημα σε τι ανταποκρίνεται ο ΓΚΠΔ. Σύμφωνα με τις απαντήσεις, 17.8% θεωρεί πως αφορά στην αυστηρότερη οριοθέτηση των διαδικασιών

συλλογής και επεξεργασίας δεδομένων, ενώ 21.8% δήλωσε ότι ανταποκρίνεται και στην ενίσχυση των δικαιωμάτων των υποκειμένων και την αύξηση των υποχρεώσεων των φορέων που συλλέγουν και διαχειρίζονται δεδομένα και την αυστηρότερη οριοθέτηση των διαδικασιών συλλογής και επεξεργασίας δεδομένων και την θέσπιση αυστηρότερων μέτρων ελέγχου συμμόρφωσης με τη νομοθεσία. Άγνοια σε υψηλό ποσοστό (41.6%) εμφανίστηκε στην ερώτηση αν γνωρίζουν οι συμμετέχοντες ποια είναι η Αρμόδια Ρυθμιστική Αρχή στην Ελλάδα, γεγονός που αποτελεί ένδειξη ότι οι χρήστες δεν γνωρίζουν ποιος δύναται να τους προστατεύσει και σε ποιόν μπορούν να απευθυνθούν.

Οι απαντήσεις για το βαθμό γνώσης δικαιωμάτων που προβλέπονται στον ΓΚΠΔ έδειξαν ότι οι χρήστες έχουν υψηλότερο βαθμό γνώσης για την απαίτηση της συγκατάθεσης, προκειμένου να χρησιμοποιηθούν τα δεδομένα τους, και για τη μορφή της συγκατάθεσης, ενώ μάλλον καλά φαίνεται να γνωρίζουν το δικαίωμα στην ενημέρωση και αυτό στη διόρθωση ανακριβών δεδομένων. Αντιθέτως χαμηλός βαθμός γνώσης καταγράφηκε για το δικαίωμα στη φορητότητα και το δικαίωμα να μην υπόκεινται σε απόφαση που λαμβάνεται αποκλειστικά στη βάση αυτοματοποιημένης επεξεργασίας. Τα ποσοστά άγνοιας των δικαιωμάτων («καθόλου») κυμάνθηκαν μεταξύ 30% (δικαίωμα στη φορητότητα) και 19% (δικαίωμα ενημέρωσης σε περίπτωση διαβίβασης δεδομένων σε τρίτους), ενώ το χαμηλότερο ποσοστό καταγράφηκε στην απαίτηση της συγκατάθεσης (5%). Το δικαίωμα στη φορητότητα δεδομένων είναι μία από τις καινοτομίες του ΓΚΠΔ, που εκτός από το γεγονός ότι αυξάνει τον έλεγχο του χρήστη στα δεδομένα του, συνιστά μια ευκαιρία για τη διαλειτουργικότητα των υπηρεσιών και την αύξηση του ανταγωνισμού μεταξύ των ψηφιακών υπηρεσιών (De Hert et al. 2018).

Τα αποτελέσματα έδειξαν, επίσης, ότι περίπου 1/5 (22.8%) των ερωτώμενων δεν γνώριζε ποτέ έχει δικαίωμα να ζητήσει από τον υπεύθυνο της επεξεργασίας τη διαγραφή προσωπικών του δεδομένων. Υψηλότερο ποσοστό απαντήσεων (21.8%) εμφανίστηκε στην περίπτωση της ανάκλησης της συγκατάθεσης. Το δικαίωμα στη διαγραφή των δεδομένων είναι ιδιαίτερα σημαντικό, καθώς ουσιαστικά αίρεται η δυνατότητα ανεξέλεγκτης ψηφιακής αναπαραγωγής των προσωπικών δεδομένων και αυξάνεται ο έλεγχος του υποκειμένου στην εμβέλεια και ροή των δεδομένων του (van Ooijen & Vrabec, 2019). Αναφορικά με το δικαίωμα στον περιορισμό της επεξεργασίας των προσωπικών δεδομένων, 29.7% των ερωτώμενων δεν γνώριζε σε ποιες περιπτώσεις έχει

το δικαίωμα αυτό, ενώ μόνο 9.9% αναγνώριζε ότι το έχει και στις τέσσερις δοθείσες ως απαντήσεις περιπτώσεις.

Αθροιστικά περισσότεροι από τους μισούς ερωτώμενους ήταν απόλυτα ή αρκετά βέβαιοι ότι ελέγχουν τα προσωπικά δεδομένα που παρέχουν online, αναγνωρίζοντας, ωστόσο, ότι μετά την παροχή των δεδομένων έχουν μερικό (56%) ή δεν έχουν κανένα έλεγχο (20%) επ' αυτών. Η διαφοροποίηση αυτή καταδεικνύει ότι τα υποκείμενα των δεδομένων μπορούν να διακρίνουν μεταξύ του σταδίου της παροχής της πληροφορίας και αυτού της πρόσβασης από άλλους, αναγνωρίζοντας ότι μετά την παροχή των δεδομένων, αυτά δεν βρίσκονται πλέον υπό τον έλεγχό τους, θέση που έχει υποστηριχθεί ήδη από τους Conger et al. (2013). Οι Brandimarte et al. (2012) έχουν δείξει ότι η αύξηση του θεωρούμενου, κι όχι του πραγματικού, ελέγχου των ατόμων στην αποκάλυψη και την πρόσβαση στις προσωπικές τους πληροφορίες, αυξάνει την προθυμία τους να αποκαλύψουν ευαίσθητες πληροφορίες και σε ένα ευρύτερο κοινό.

Η αναγνώριση των υποκειμένων των δεδομένων ότι τα δεδομένα τους ελέγχονται από άλλους καταγράφηκε και στη σχετική ερώτηση για τις ανησυχίες ιδιωτικότητας. Η πλειοψηφία των ερωτώμενων δήλωσε (82.2%) δήλωσε «πολύ ανήσυχος» και «αρκετά ανήσυχος», ενώ υψηλά ήταν και τα επίπεδα ανησυχίας για το γεγονός ότι κυβερνητικοί φορείς συλλέγουν προσωπικά δεδομένα σε μεγάλη κλίμακα με σκοπό την εθνική ασφάλεια. Τα αποτελέσματα έδειξαν ότι οι μισοί σχεδόν (49%) ήταν αρκετά ανήσυχοι και 22% πολύ ανήσυχοι. Οι ανησυχίες των υποκειμένων των δεδομένων αυξήθηκαν ακόμη περισσότερο όταν ρωτήθηκαν πόσο άνετα νιώθουν με το γεγονός ότι οι ιστοσελίδες εταιρειών χρησιμοποιούν την πληροφορία για την online δραστηριότητά τους, ώστε να διαμορφώσουν περιεχόμενο που ανταποκρίνεται στις προτιμήσεις τους. Από τους ερωτώμενους, «όχι ιδιαίτερα άνετα» δήλωσε 40.6% και «καθόλου άνετα» 48.5%. Ανησυχίες καταγράφηκαν και σε σχέση με το θέμα της αξιοποίησης προσωπικών δεδομένων από δημόσιους ή ιδιωτικούς φορείς για διαφορετικούς λόγους από αυτούς για τους οποίους είχαν συλλεγεί αρχικά, χωρίς ενημέρωση των υποκειμένων των δεδομένων. Συγκεκριμένα, 39.6% των ερωτώμενων δήλωσαν «πολύ ανήσυχοι» και 49.5% «αρκετά». Ιδιαίτερος προβληματισμός καταγράφηκε και για το γεγονός ότι δημοφιλείς μηχανές αναζήτησης, όπως η Google, καταγράφουν το ιστορικό περιήγησης των χρηστών. Μόνο 3% των ερωτώμενων δήλωσε ότι δεν τους έχει απασχολήσει το θέμα, καθόλου ανήσυχοι δήλωσαν 4% και όχι ιδιαίτερα ανήσυχοι 9.9%. Με βάση τα

παραπάνω, φαίνεται ότι σε όλες τις υπό εξέταση περιπτώσεις τα ποσοστά ανησυχούντων είναι αρκετά υψηλά, γεγονός ενθαρρυντικό για την ανάληψη από τους χρήστες μέτρων προστασίας της ιδιωτικότητάς τους.

Με εξαίρεση έναν/μια συμμετέχοντα/ουσα, όλοι οι υπόλοιποι απάντησαν ότι θα ήθελαν να έχουν πληροφόρηση στην περίπτωση που χαθούν ή κλαπούν τα προσωπικά τους δεδομένα και πάνω από τους μισούς (51.5%) δήλωσαν ότι ανησυχούν εξίσου για την απώλεια δεδομένων αποθηκευμένων στον Η/Υ, τις κινητές συσκευές και online/cloud. Οι κίνδυνοι που δήλωσαν οι χρήστες σε περίπτωση κλοπής των δεδομένων τους εστιάζουν περισσότερο σε αξιοποίηση αυτών για λόγους απάτης, ενώ έπονται οι κίνδυνοι για την χρησιμοποίηση των πληροφοριών τους χωρίς να το γνωρίζουν ή τη διανομή τους σε τρίτους χωρίς τη συγκατάθεσή τους. Πολύ χαμηλότερα ποσοστά καταγράφηκαν για τον κίνδυνο παρερμηνείας των απόψεων και της συμπεριφοράς τους ή για την αποστολή ανεπιθύμητου διαφημιστικού υλικού.

Το μεγαλύτερο ποσοστό των ερωτώμενων (64.4%) διαβάζει μερικώς τις πολιτικές απορρήτου, οι δε λόγοι για την μερική ανάγνωση εστιάζουν στην έκταση του κειμένου (73.4%) και στο δυσνόητο περιεχόμενο (55.4%), γεγονός που υποδεικνύει την ανάγκη για σαφή και σύντομα κείμενα από πλευράς των παρόχων. Ένα μικρό ποσοστό (13.9%) δήλωσε ότι αρκείται να βλέπει ότι υπάρχει πολιτική απορρήτου, πράγμα που δείχνει εμπιστοσύνη στους παρόχους. Σε κάθε περίπτωση, η μερική ή η μη ανάγνωση των πολιτικών απορρήτου έχει αναγνωριστεί βιβλιογραφικά ότι συνιστά κίνδυνο.

Συνδυασμός επιλογών καταγράφηκε ως απάντηση στην ερώτηση πού θα πρέπει να απευθυνθούν οι χρήστες σε περίπτωση παραβίασης των προσωπικών τους δεδομένων. Από τους ερωτώμενους, 11.9% δήλωσαν ότι δεν γνωρίζουν, ενώ ως ισχυρότερη καταγράφηκε (28.7%) η επιλογή «Αρμόδια Ρυθμιστική Αρχή». Η σύγκυση αυτή ενδεχομένως σχετίζεται με άγνοια των αρμοδιοτήτων που έχει κάθε ένας από τους φορείς που προτάθηκαν ως απάντηση, άρα άγνοια της νομοθεσίας σχετικά με την άσκηση ένδικων μέσων.

Οι ερωτώμενοι δήλωσαν υψηλό βαθμό γνώσης σε σχέση με την απαίτηση της συγκατάθεσης, ωστόσο 25% δεν είναι βέβαιοι ότι την παρέχουν με ρητό τρόπο και 21% δεν το κάνει, πράγμα που σημαίνει ότι αν και το δικαίωμα είναι γνωστό, μάλλον δεν

ασκείται ορθά. Επιπλέον, αν και της παροχής της συγκατάθεσης πρέπει να προηγείται ενημέρωση των υποκείμενων των δεδομένων για τις συνθήκες συλλογής και επεξεργασίας των δεδομένων τους, οι απαντήσεις των ερωτώμενων έδειξαν, σε υψηλά ποσοστά, ότι αυτό συμβαίνει «ορισμένες φορές» (37.6%) ή «σπάνια» (39.6%).

Αν και πάνω από τους μισούς ερωτώμενους (54%) δεν είχαν ή είχαν μικρή γνώση του δικαιώματος στη φορητότητα, η πλειονότητα των ερωτώμενων έκρινε τη δυνατότητα της φορητότητας δεδομένων πολύ σημαντική (38.6%) ή αρκετά σημαντική (36.6%), γεγονός που μάλλον δείχνει ότι αντιλαμβάνονται το δικαίωμα αυτό ως μια δυνατότητα αύξησης του ελέγχου στα δεδομένα τους.

Στην τελευταία ερώτηση του ερωτηματολογίου, οι συμμετέχοντες κλήθηκαν να δηλώσουν τη συμφωνία ή διαφωνία τους με έξι θέσεις : α) Είμαι βέβαιος/η ότι τα προσωπικά δεδομένα που παρέχω δεν αξιοποιηθούν από κανέναν άλλο, β) Γνωρίζω καλά τη νομοθεσία για την προστασία των δεδομένων μου για να προστατεύσω τον εαυτό μου, γ) Εμπιστεύομαι τους παρόχους υπηρεσιών για να προστατεύουν τα δεδομένα μου, δ) Η νομοθεσία και οι ρυθμιστικές αρχές προστατεύουν πλήρως τα προσωπικά μου δεδομένα, ε) Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online, και στ) Οι κυβερνήσεις προστατεύουν τα δεδομένα μου. Οι θέσεις αυτές ελέγχουν τη στάση των ερωτώμενων απέναντι στους παρόχους, τις κυβερνήσεις και τη νομοθεσία.

Σε καμία από τις θέσεις δεν καταγράφηκαν ποσοστά συμφωνίας ή απόλυτης συμφωνίας υψηλότερα από τα ποσοστά διαφωνίας ή απόλυτης διαφωνίας και μάλιστα σε 5 από τις 6, τα ποσοστά συμφωνίας ή απόλυτης συμφωνίας ήταν επίσης χαμηλότερα από τα ποσοστά της απάντησης «ούτε συμφωνώ, ούτε διαφωνώ». Οι ερωτώμενοι, σε ποσοστό άνω του 50%, δεν πιστεύουν ότι οι κυβερνήσεις προστατεύουν τα δεδομένα τους (61.4%) και δεν εμπιστεύονται τους παρόχους για την προστασία των δεδομένων τους (52.4%), ενώ σε μικρότερο ποσοστό (40.6%) δήλωσαν ότι η νομοθεσία και οι ρυθμιστικές αρχές τους δεν προστατεύουν. Τα αποτελέσματα αυτά δείχνουν την αναμενόμενη έλλειψη εμπιστοσύνης σε παρόχους, αλλά ταυτόχρονα, καθώς η παρούσα έρευνα διερευνά το ΓΚΠΔ, αποτελούν ισχυρές ενδείξεις για απουσία εμπιστοσύνης στη νέα νομοθεσία, τις κυβερνήσεις που είναι υπεύθυνες για την υλοποίησή της και τις Αρχές που έχουν την ευθύνη του ελέγχου συμμόρφωσης.

Από την άλλη πλευρά, οι ερωτώμενοι αναγνώρισαν ότι τα δεδομένα τους μπορούν να αξιοποιηθούν από άλλους (53.5%), επιβεβαιώνοντας αποτελέσματα προηγούμενων ερωτήσεων σε σχέση με τον έλεγχο της πληροφορίας. Η κατανομή των απαντήσεων στην δήλωση που αφορά την καλή γνώση της νομοθεσίας (26.7% «συμφωνώ» και «συμφωνώ απόλυτα, 34.7% «ούτε συμφωνώ, ούτε διαφωνώ» και 38.7% «διαφωνώ» και «διαφωνώ απόλυτα») δείχνει την αμφιβολία των χρηστών, επιβεβαιώνοντας έτσι και τα αποτελέσματα της έρευνας που σχετίζονται με το βαθμό γνώσης των επιμέρους δικαιωμάτων τους. Τέλος, η σχετικά ισόποση κατανομή απαντήσεων στη δήλωση ότι για την επίτευξη της προστασίας αρκεί η προσοχή στα δεδομένα που παρέχονται online είναι ενδεικτική του ότι ούτε οι ατομικές στρατηγικές προστασίας για τη ρύθμιση της ιδιωτικότητάς τους και την προστασία των δεδομένων τους θεωρούνται αρκετά αποτελεσματικές.

Η εφαρμογή του ΓΚΠΔ είναι μια σύνθετη διαδικασία και απαιτεί μια ολιστική προσέγγιση με αναφορά σε ανθρώπους, διαδικασίες και συστήματα (τεχνολογία) (Datoo 2018) καθώς και οι τρεις συνιστώσες εμπλέκονται, με διαφορετικό βέβαια τρόπο, στην επεξεργασία των προσωπικών δεδομένων. Καθώς η νέα νομοθεσία έχει φροντίσει να εισαγάγει νέες υποχρεώσεις για τους φορείς που διαχειρίζονται τα δεδομένα των υποκειμένων και σαφείς διαδικασίες για τη συλλογή και επεξεργασία αυτών, ρυθμίζοντας επιπλέον τρόπους ελέγχου συμμόρφωσης με τη νομοθεσία αλλά και θεσπίζοντας προληπτικούς ελέγχους, τα υποκείμενα των δεδομένων οφείλουν από την πλευρά τους να έχουν πολύ καλή γνώση των δικαιωμάτων τους αλλά και γενικότερα των προβλέψεων του ΓΚΠΔ. Αυτό συνάδει με τη θέση των Trepte κ.α. (2015) και του Park (2011) ότι η γνώση για τη νομοθεσία της προστασίας δεδομένων και τους νομικούς περιορισμούς που επιβάλλονται στις εταιρείες, αλλά και η γνώση των πρακτικών συλλογής και των τεχνικών επεξεργασίας δεδομένων συμβάλλει ώστε τα υποκείμενα των δεδομένων να κατορθώσουν να ελέγξουν την προστασία των δεδομένων τους και να βελτιστοποιήσουν την ιδιωτικότητά τους.

Τα αποτελέσματα της έρευνας κατέδειξαν διακυμάνσεις στο βαθμό γνώσης των υποκειμένων των δεδομένων για τα δικαιώματά τους, χωρίς, ωστόσο, να είναι γνωστές οι αιτίες που τις προκαλούν. Μελλοντική έρευνα θα πρέπει να εστιάσει στην αναζήτηση των παραγόντων εκείνων που επιδρούν στο βαθμό γνώσης των δικαιωμάτων, ενδεχομένως σχετιζόμενων με τον τρόπο ιεράρχησης των δικαιωμάτων σε ατομικό

επίπεδο, με την έμφαση που δίνεται σε συγκεκριμένα δικαιώματα από τις πηγές πληροφόρησης ή με προηγούμενες εμπειρίες των υποκειμένων. Επιπλέον, θα πρέπει να διερευνηθεί η απόκλιση που φαίνεται να εμφανίζεται ανάμεσα στη γνώση των δικαιωμάτων -στο βαθμό που καταδείχθηκε- και στη συμπεριφορά των υποκειμένων για παράδειγμα στο θέμα της παροχής της συγκατάθεσης, ώστε να διαπιστωθεί αν συνιστά ένα παράδοξο, μια αντίφαση ανάμεσα στη γνώση και τη συμπεριφορά, κατ' αναλογία με το ήδη αναγνωρισμένο βιβλιογραφικά Privacy Paradox (αντίφαση ανάμεσα στην πρόθεση στάσης και την εκδηλούμενη συμπεριφορά (Acquisti & Gross 2006, Dienlin & Trepte, 2015), ή αν η συμπεριφορά δεν προσδιορίζεται τόσο από τη γνώση, αλλά από τη συνήθεια της πρακτικής (habitus). Είναι προφανές, επίσης, ότι μια ολοκληρωμένη αποτύπωση της γνώσης των υποκειμένων των δεδομένων για τα δικαιώματά τους, όπως προβλέπονται στον ΓΚΠΔ, πρέπει να περιλαμβάνει αντίστοιχες έρευνες και σε άλλες χώρες –μέλη της Ευρωπαϊκής Ένωσης,

Αν και τα αποτελέσματα της παρούσας έρευνας δεν μπορούν να γενικευθούν, όπως εξηγήθηκε στο κεφάλαιο της Μεθοδολογίας, ωστόσο παρέχουν ιδιαίτερα ισχυρές ενδείξεις ότι απαιτείται μέριμνα για την ενίσχυση της γνώσης των υποκειμένων των δεδομένων σε σχέση με τη νομοθεσία, τα δικαιώματά τους και την προστασία των δεδομένων τους. Έρευνες έχουν δείξει ότι η ενίσχυση της επίγνωσης των χρηστών για το βαθμό της γνώσης τους σε σχέση με την προστασία των δεδομένων τους και την ιδιωτικότητά τους έχει θετική επίδραση στην ανάληψη από τα ίδια τα υποκείμενα συμπεριφοράς προστασίας (Park 2011, Moll, Pieschl, & Bromme 2014). Ιδιαίτερα σημαντικός είναι, έτσι, ο ρόλος των εκπαιδευτικών παρεμβάσεων ή των ενημερωτικών εκστρατειών στην ενίσχυση της γνώσης των υποκειμένων των δεδομένων για τη νομοθεσία και τα δικαιώματά τους. Ειδικότερα, η συμπερίληψη της νομοθεσίας στο πλαίσιο εκπαιδευτικών παρεμβάσεων κρίνεται μείζονος σημασίας (Sideri, Kitsiou, Tzortzaki, Kalloniatis & Gritzalis 2017) για την κατανόηση, από πλευράς των υποκειμένων, της σημασίας προστασίας των προσωπικών τους δεδομένων και με δική τους ευθύνη.

Ο ΓΚΠΔ διαμόρφωσε ένα νέο πλαίσιο στην προστασία των προσωπικών δεδομένων, χωρίς να απομακρυνθεί από τις προηγούμενες θεσπισθείσες αρχές, αλλά δίνοντας ιδιαίτερη έμφαση στην δυνατότητα των υποκειμένων των δεδομένων να έχουν μεγαλύτερο έλεγχο επ' αυτών, με την ενίσχυση των δικαιωμάτων τους. Αν η εφαρμογή του ΓΚΠΔ αποτελεί ευθύνη των μελών κρατών της Ευρωπαϊκής Ένωσης, η εναρμόνιση

με αυτόν ευθύνη όσων διαχειρίζονται προσωπικά δεδομένα και η παρακολούθηση της εφαρμογής όπως και η αντιμετώπιση περιστατικών παραβίασης αρμοδιότητα των Αρχών, η δημιουργία ενός συνεκτικού τοπίου προστασίας των προσωπικών δεδομένων ολοκληρώνεται με ενέργειες προστασίας των δεδομένων από τα ίδια τα υποκείμενα. Και τούτο απαιτεί γνώση των δικαιωμάτων και άσκηση αυτών.

Βιβλιογραφία

- Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on The Facebook. In G. Danezis & P. Golle (eds), *Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET '06)* (pp. 273-290). UK: Springer
- Babbie, E. (2011). *Εισαγωγή στην Κοινωνική Έρευνα*. Αθήνα : Κριτική
- Baek, Y.M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, 38, 33–42.
- Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. In: *Proceedings of the 29th International Conference on Information Systems* (pp. 1-19). Paris: AIS Electronic Library. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1209&context=icis2008> [Πρόσβαση: 08.04.2019].
- Benson, V., Saridakis, G. & Tennakoon, H. (2015). Information disclosure of social media users. Does control over personal information, user awareness and security notices matter?, *Information Technology & People*, 28 (3), 426-441.
- Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, 18(1), 21–28.
- Brandimarte, L., Acquisti, A. & Loewenstein, G. (2012). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4 (3) 340-347.
- Buschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y. & Elger, B. (2014). Protecting Human Health and Security in Digital Europe: How to Deal with the “Privacy Paradox”?, *Sci Eng. Ethics*, 20, 639–658.
- Cadogan, R.A. (2011). An imbalance of power: the readability of internet privacy policies. *Journal of Business & Economics Research*, 2 (3), 49-62.
- Cebrian J.L. (2000). *Το δίκτυο*. Αθήνα : Στάχυ.
- Cecere, G., Le Guel, F. & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting & Social Change*, 96, 277–287.
- Cohen, L. & Manion, L. (1994). *Μεθοδολογία Εκπαιδευτικής Έρευνας*. Αθήνα: Μεταίχμιο.

- Conger, S., Pratt, J.H. & Loch, K.D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23 (5), 401-417.
- Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review*, 34 (2), 234-243.
- Datoo, A. (2018). Data in the post-GDPR world. *Computer Fraud and Security*, 9, 17-18.
- De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*, 34(2), 193-203.
- Dienlin, T. & Trepte, S. (2015). Putting the Social (Psychology) into Social Media Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur. J. Soc. Psychol.*, 45, 285-297.
- Ευρωπαϊκό Κοινοβούλιο (2016). *Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)*. <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL> [πρόσβαση: 30.03.2019].
- Economist (2017, May 5). *The world's most valuable resource is no longer oil, but data*. <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> [πρόσβαση: 02.04.2019]
- European Commission (2015). *Special Eurobarometer 431. Data Protection Report, E.U.* http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf [πρόσβαση: 02.04.2019]
- European Union Agency for Fundamental Rights, 2018. *Handbook on European data protection law*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf [πρόσβαση: 28.03.2019].
- Ζαφειρόπουλος, Κ. (2015). *Πώς γίνεται μια επιστημονική εργασία; Επιστημονική Έρευνα και συγγραφή εργασιών*. Αθήνα : Κριτική
- Hoofnagle, C. J., & Urban, J. M. (2014). AlanWestin's privacy homo economicus. *Wake Forest Law Review*, 49, 261-317.
- Hughes, D. (2015). Two concepts of privacy. *Computer law & security review*, 31, 527-537.

- Javeau, C. (1996). *Η έρευνα με ερωτηματολόγιο*. Αθήνα : Τυπωθήτω.
- Κάλλας, Γ. (2006). *Η κοινωνία της πληροφορίας και ο ρόλος των κοινωνικών επιστημών*. Αθήνα: Νεφέλη.
- Kelley, P. G., Cranor, L. F. & Sadeh, N. (2013). Privacy as part of the app decision-making process. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 3393-3402). Paris, France : ACM.
- Μήτρου, Α. (2002). *Το Δίκαιο στην Κοινωνία της Πληροφορίας*. Αθήνα : εκδ. Σάκκουλα.
- Μήτρου, Α. (2010). Προστασία της ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες – Η νομική διάσταση. Σε: Λαμπρινουδάκης, Κ., Μήτρου, Α., Γκριτζαλής, Σ., & Κάτσικας, Σ. (επιμ.). *Ιδιωτικότητα και Τεχνολογίες Πληροφορικής και Επικοινωνιών - Τεχνικά και Νομικά Ζητήματα* (σσ. 505-552). Αθήνα: Παπασωτηρίου.
- Marwick, A.E., Murgia-Diaz, D. & Palfrey, J.G. (2010). Youth, Privacy and Reputation (Literature Review). UK, Cambridge: Berkman <https://clalliance.org/wp-content/uploads/files/YouthPrivacyReputationBERKMAN.pdf> [πρόσβαση: 21.04.2019].
- Marx, G.T. (2001). Murky Conceptual Waters: The Public and the Private. *Ethics and Information Technology*, 3 (3), 157-169.
- Milne, G. R. & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18 (3), 15-29.
- Miltgen, C. L. and Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, 23, 103–125.
- Moll, R., Pieschl, St. & Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers on Human Behavior*, 41, 212-219.
- Νόμος 2472/97. Προστασία του ατόμου από την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDO MENA/FILES/2472_97_JUNE2013.PDF [πρόσβαση: 03.04.2019].
- Oppenheim, A. (1992). *Questionnaire Design, Interviewing and Attitude Measurement*. London: Pinter

- Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40 (2), 215–236
- Posey, C., Lowry, P.B., Roberts, T.L. & Ellis, T.S. (2010). Proposing the online community self- disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, 19 (2), 181-195
- Pouillet, Y. (2018). Is the general data protection regulation the solution? *Computer Law and Security Review*, 34 (4), 773–778.
- Proctor, R.W., Athar Ali, M. & Vu, K-P. L. (2008) Examining Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction*, 24 (3), 307-328.
- Ρούσσοσ, Π. & Τσαούσης, Γ. (2011). *Στατιστική στις Επιστήμες της Συμπεριφοράς με τη χρήση SPSS*. Αθήνα : Τόπος.
- Ragnedda, M. (2011). Social control and surveillance in the society of consumers. *Int. J. Sociol. Anthropol.* 3(6), 180–188.
- Research Methodology (2013). *Exploratory Research*. <https://research-methodology.net/research-methodology/research-design/exploratory-research/> [Πρόσβαση: 28.03.2019].
- Σιδερί, Μ., Κίτσιου, Α., Τζωρτζάκη, Ε., Καλλονιάτης, Χ. & Γκριτζαλής Σ., (2017). Προστασία της Ιδιωτικότητας σε Ψηφιακά Κοινωνικά Δίκτυα, Μια αναγκαία για τη διατήρηση της κοινωνικής συνοχής στην Κοινωνία της Πληροφορίας; Σε: Παπαβασιλείου, Β., Φώκιαλη, Π., Νικολάου, Ε., Μαντζανος, Δ. & Καϊλα Μ. (επιμ.) *Κοινωνική και Πολιτισμική Βιωσιμότητα* (σσ. 134-174). Ελλάδα, Ρόδος: ΠΜΣ Περιβαλλοντική Εκπαίδευση. <http://www.pse.aegean.gr/pms-pe/media/E%20-%20BOOK.pdf> [Πρόσβαση: 28.03.2019].
- Sideri, M., Kitsiou, A., Tzortzaki, E., Kalloniatis, C. & Gritzalis, S. (2017). “I have learned that I must think twice before...”. An educational intervention for enhancing students’ privacy awareness in Facebook. In : S. Katsikas & V. Zorkadis, (eds) *Proceedings of the 7th International Conference on E-Democracy-Privacy-Preserving, Secure, Intelligent E-Government Systems*, (pp. 79-94). Cham, Switzerland: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-71117-1_6 [Πρόσβαση 1.5.2019].
- Sobolewski, M., Mazur, J., & Paliński, M. (2017). GDPR: A step towards a user-centric internet? *Intereconomics*, 52 (4), 207–213.
- Taddicken, M. (2014). The ‘Privacy Paradox in the Social Web: The Impact of Privacy Concerns, Individual Characteristics and the Perceived Social Relevance on Different

Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, 19 (2), 248-273.

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

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In : Gutwirth, S., Leenes, R. & de Hert, P. (Eds), *Reforming European Data Protection Law* (pp. pp. 333-365). Brussels : Springer.

Warren, S. & Brandeis, L. (1890). The Rights to Privacy. *Harvard Law Review*, 4 (5), 193-220.

Van Dijck, J. (2013). *The Culture of Connectivity: a Critical History of Social Media*. UK: Oxford University Press.

van Ooijen, I. & Vrabec, H.U (2019). Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, 42, 91–107.

Ziegele, M. & Quiring, O. (2011). Privacy in Social Network Sites. In: Trepte, S. & Reinecke, L. (Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web* (pp.175-189). Germany, Berlin: Springer.

Παράρτημα Α

Σύγκριση Κανονισμού 2016/679/ΕΕ με Οδηγία 95/46/ΕΕ

	Οδ. 95/46 ΕΕ	2016/769 ΕΕ	Νέα δεδομένα (Tikkinen-Piri, Rohunen, & Markkula 2018).
Γενικές Προβλέψεις και αρχές	Ορισμοί (άρθρο 2), εφαρμοστέο εθνικό δίκαιο (άρθρο 4), αρχές σχετικά με την ποιότητα των δεδομένων (άρθρο 6), κριτήρια για νόμιμη επεξεργασία δεδομένων (άρθρο 7) και επεξεργασία ειδικών κατηγοριών δεδομένων (άρθρο 8)	Άρθρα 1-11	<ul style="list-style-type: none"> • Εκτεταμένη εδαφική εμβέλεια • Νέοι ορισμοί (π.χ. ψευδωνυμοποίηση, δεδομένα γενετικά, βιομετρικά, υγείας) • Νέες προβλέψεις και αρχές (πχ. διαφάνεια επεξεργασίας δεδομένων, λογοδοσία και επεξεργασία που δεν απαιτεί ταυτοποίηση) • Διευκρίνιση ή εξειδίκευση προβλέψεων και αρχών (πχ. αρχή της ελαχιστοποίησης των δεδομένων, προϋποθέσεις συναίνεσης και νόμιμη επεξεργασία δεδομένων) • Προσθήκη προϋποθέσεων για τη συγκατάθεση ενός παιδιού (συγκατάθεση ή άδεια γονέα ή κηδεμόνα για παιδί κάτω των 16 ετών)
Διαφάνεια και τυπικότητα	Το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων στα δεδομένα (άρθρο 12)	Άρθρο 12	<ul style="list-style-type: none"> • Νέες υποχρεώσεις των υπεύθυνων επεξεργασίας (πχ. παροχή εύκολα προσβάσιμων και κατανοητών πληροφοριών σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρόβλεψη διαδικασιών και μηχανισμών για την

			παροχή δυνατότητας στο υποκείμενο να ασκήσει τα δικαιώματά του)
Πληροφορίες και πρόσβαση σε προσωπικά δεδομένα	Πληροφορίες που πρέπει να δίνονται στο υποκείμενο των δεδομένων (άρθρα 10-11) και το δικαίωμα πρόσβασης των υποκειμένων στα δεδομένα (άρθρο 12α)	Άρθρα 13-15	<ul style="list-style-type: none"> • Εξειδίκευση υποχρέωσης του υπεύθυνου επεξεργασίας για παροχή πρόσθετης πληροφόρησης στο υποκείμενο των δεδομένων σχετικά με τον υπεύθυνο επεξεργασίας, τα δικαιώματά του υποκειμένου των δεδομένων και τη διαβίβαση δεδομένων σε τρίτες χώρες • Πρόσθετες πληροφοριακές απαιτήσεις σχετικά με το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων στα δεδομένα του
Διόρθωση και διαγραφή	Δικαίωμα πρόσβασης (άρθρο 12β-γ)	Άρθρα 16-20	<ul style="list-style-type: none"> • Καθορισμός δικαιωμάτων υποκειμένων των δεδομένων στη διόρθωση, τη διαγραφή και τον περιορισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (όροι άσκησης του δικαιώματος στη λήθη και του δικαιώματος περιορισμού επεξεργασίας) • Νέο δικαίωμα του υποκειμένου των δεδομένων: φορητότητα δεδομένων
Δικαίωμα αντικρούσεως και αυτοματοποιημένη λήψη απόφασης	Το δικαίωμα του υποκειμένου των δεδομένων στην υποβολή ενστάσεων (άρθρο 14) και αυτοματοποιημένες ατομικές αποφάσεις (άρθρο 15)	Άρθρα 21-22	<ul style="list-style-type: none"> • Προσδιορισμός δικαιώματος υποβολής αντιρρήσεων στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της κατάρτισης προφίλ. • Εξειδίκευση σχετικά με το δικαίωμα του υποκειμένου των

			<p>δεδομένων να μην υπόκειται σε απόφαση που βασίζεται σε αυτοματοποιημένη επεξεργασία.</p>
<p>Γενικές υποχρεώσεις</p>	<p>Εμπιστευτικότητα της επεξεργασίας (Άρθρο 16), την ασφάλεια της επεξεργασίας (άρθρο 17), κοινοποίηση (άρθρο 18) και περιεχόμενο της κοινοποίησης (άρθρο 19)</p>	<p>Άρθρα 24-31</p>	<ul style="list-style-type: none"> • Νέες υποχρεώσεις του υπεύθυνου επεξεργασίας (αρχές προστασίας δεδομένων από το σχεδιασμό και από προεπιλογή) • Διευκρινίσεις σχετικά με τις ευθύνες και τις υποχρεώσεις των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία • Νέες υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία (πχ. τήρηση μητρώων των δραστηριοτήτων επεξεργασίας, συνεργασία με την εποπτική αρχή)
<p>Ασφάλεια των προσωπικών δεδομένων</p>	<p>Ασφάλεια επεξεργασίας (άρθρο 17).</p>	<p>Άρθρα 32-34</p>	<ul style="list-style-type: none"> • Επέκταση υποχρέωσης εκτελούντων την επεξεργασία (λήψη μέτρων για την ασφάλεια της επεξεργασίας δεδομένων) • Νέα υποχρέωση του υπεύθυνου επεξεργασίας: κοινοποίηση παραβίασης των προσωπικών δεδομένων στην εποπτική αρχή και στο υποκείμενο των δεδομένων • Νέα υποχρέωση του εκτελούντος την επεξεργασία: κοινοποίηση παραβίασης των προσωπικών δεδομένων στον υπεύθυνο επεξεργασίας

Αξιολόγηση αντικτύπου προστασίας δεδομένων και προηγούμενη διαβούλευση	Προηγούμενοι έλεγχοι (άρθρο 20)	Άρθρα 35-36	<ul style="list-style-type: none"> • Νέα υποχρέωση των υπευθύνων επεξεργασίας για την αξιολόγηση των επιπτώσεων προστασίας των δεδομένων πριν από πιθανή επικίνδυνη επεξεργασία • Απλούστευση σε σχέση με την υποχρέωση των υπευθύνων επεξεργασίας να λαμβάνουν εξουσιοδότηση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
Υπεύθυνος προστασίας δεδομένων (DPO)	Υποχρέωση κοινοποίησης στην Εποπτική Αρχή (άρθρο 18)	Άρθρα 37-39	<ul style="list-style-type: none"> • Νέα υποχρέωση του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία ο ορισμός υπεύθυνου προστασίας δεδομένων
Κώδικες συμπεριφοράς και πιστοποίηση	Κώδικες συμπεριφοράς (άρθρο 27)	Άρθρα 40-43	<ul style="list-style-type: none"> • Απλοποιήσεις σχετικά με την έγκριση κωδίκων δεοντολογίας. • Νέα μέσα για την απόδειξη της συμμόρφωσης των διαδικασιών επεξεργασίας με το ΓΚΠΔ (μηχανισμοί πιστοποίησης προστασίας δεδομένων, σφραγίδες)
Μεταφορά δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή σε διεθνείς οργανισμούς	Αρχές (άρθρο 25) και παρεκκλίσεις (άρθρο 26)	Άρθρα 44-49	<ul style="list-style-type: none"> • Νέες συνθήκες για την ασφαλή διαβίβαση των προσωπικών δεδομένων
Διορθωτικά μέτρα, ευθύνη και κυρώσεις	Διορθωτικά μέτρα (άρθρο 22), ευθύνη (άρθρο 23) και κυρώσεις (άρθρο 24)	Άρθρα 77-84	<ul style="list-style-type: none"> • Εξειδίκευση αναφορικά με το δικαίωμα του υποκειμένου των δεδομένων σε ένδικα μέσα • Επέκταση ευθύνης του υπεύθυνου της επεξεργασίας και του εκτελούντος την επεξεργασία για τη ζημία

			<p>που προκλήθηκε στο υποκείμενο των δεδομένων με επεξεργασία που παραβιάζει τον ΓΚΠΔ</p> <ul style="list-style-type: none">• Αποσαφήνιση της ευθύνης των από κοινού υπευθύνων επεξεργασίας και των από κοινού εκτελούντων την επεξεργασία.• Διοικητικά πρόστιμα που επιβάλλονται στον υπεύθυνο της επεξεργασίας και τον εκτελούντα την επεξεργασία.
--	--	--	---

Παράρτημα Β Ερωτηματολόγιο

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ για τον ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΓΚΠΔ)

Στο πλαίσιο έρευνας που διεξάγεται για την εκπόνηση διπλωματικής διατριβής με θέμα «Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), προστασία της ιδιωτικότητας και δικαιώματα των χρηστών» στο Πρόγραμμα Μεταπτυχιακών Σπουδών «Κοινωνικά Πληροφοριακά Συστήματα» του Ανοικτού Πανεπιστημίου Κύπρου παρακαλούμε για την εθελοντική συμβολή σας.

Η έρευνα αφορά στη διερεύνηση της γνώσης ενηλίκων χρηστών του Διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης (ΜΚΔ) σχετικά με τις ρυθμίσεις που φέρνει ο Γενικός Κανονισμός Προστασίας Δεδομένων στο θέμα της συλλογής και διαχείρισης, από οργανισμούς, φορείς και εταιρείες, προσωπικών δεδομένων και στο θέμα των δικαιωμάτων των υποκειμένων των δεδομένων.

Για τη διεξαγωγή της έρευνας θα χρειαστεί να αφιερώσετε 15 λεπτά από το χρόνο σας, ώστε να συμπληρώσετε το ακόλουθο ερωτηματολόγιο.

Επισημαίνεται ότι οι απαντήσεις είναι απολύτως εμπιστευτικές και ανώνυμες.

Ευχαριστούμε εκ των προτέρων για τη συμβολή σας.

Α. Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

1. Πώς λάβατε πληροφόρηση για τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ);

- Από τα ΜΜΕ
- Από το Διαδίκτυο
- Από προσωπική ενασχόληση
- Από συζήτηση με κάποιον/ους άλλο/ους

2. Η εφαρμογή του ΓΚΠΔ αποτελεί ευθύνη σε επίπεδο:

Ευρωπαϊκό Επίπεδο Εθνικό Επίπεδο Περιφερειακό ή Τοπικό Επίπεδο Δεν γνωρίζω

3. Σε ποια από τα παρακάτω ζητήματα θεωρείτε ότι ανταποκρίνεται ο ΓΚΠΔ (μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις);

Στην ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων

Στην αύξηση των υποχρεώσεων των φορέων που συλλέγουν και διαχειρίζονται δεδομένα

Στην αυστηρότερη οριοθέτηση των διαδικασιών συλλογής και επεξεργασίας δεδομένων

Στην θέσπιση αυστηρότερων μέτρων ελέγχου συμμόρφωσης με τη νομοθεσία

4. Γνωρίζετε ποια είναι η Αρμόδια Ρυθμιστική Αρχή στη χώρα μας, που είναι υπεύθυνη για την προστασία των δικαιωμάτων σας σχετικά με τα προσωπικά σας δεδομένα;

Ναι Όχι

B. Τα δικαιώματα των υποκειμένων των δεδομένων

1. Σε ποιο βαθμό γνωρίζετε ότι ο διαχειριστής των δεδομένων* οφείλει να σας ενημερώσει, σε εύλογο χρονικό διάστημα, με σαφή τρόπο για την επεξεργασία στην οποία πρόκειται να υποβληθούν τα δεδομένα σας και για τα δικαιώματά σας;

1 2 3 4 5

Καθόλου

Άριστα

2. Σε ποιο βαθμό γνωρίζετε ότι έχετε το δικαίωμα να απαιτήσετε από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών προσωπικών δεδομένων σας;

1 2 3 4 5

Καθόλου

Άριστα

3. Σε ποιο βαθμό γνωρίζετε ότι απαιτείται η συγκατάθεσή σας για την χρήση των προσωπικών σας δεδομένων;

1 2 3 4 5

Καθόλου

Άριστα

- γ) όταν ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από εσάς για την θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων
- δ) όταν έχετε αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερσχύουν έναντι όλων των δικών σας λόγων.
- ε) δεν γνωρίζω

Γ. Κίνδυνοι για τα προσωπικά δεδομένα και τρόποι προστασίας

Γ.1 Έλεγχος Προσωπικών δεδομένων και κίνδυνοι

1. Ελέγχω τα προσωπικά δεδομένα που παρέχω online

- Είμαι απόλυτα βέβαιος/η Είμαι αρκετά βέβαιος/η Δεν είμαι ιδιαίτερα βέβαιος/η Δεν είμαι καθόλου βέβαιος/η Δεν γνωρίζω

2. Κατά πόσον νιώθετε ότι έχετε τον έλεγχο της πληροφορίας που παρέχετε online; (π.χ. την δυνατότητα να διορθώσετε, να αλλάξετε ή και να διαγράψετε αυτήν την πληροφορία;)

- Πλήρης Έλεγχος Μερικός έλεγχος Καθόλου έλεγχος Εξαρτάται Δεν Γνωρίζω

3. Κατά πόσον ανησυχείτε για το ότι άλλοι έχουν τον έλεγχο της πληροφορίας που παρέχετε online; Είστε:

- Πολύ ανήσυχος Αρκετά Ανήσυχος Όχι ιδιαίτερα ανήσυχος Καθόλου Ανήσυχος Δεν γνωρίζω

4. Σας ανησυχούν οι αποκαλύψεις ότι κυβερνητικοί φορείς συλλέγουν προσωπικά δεδομένα σε μεγάλη κλίμακα με σκοπό την εθνική ασφάλεια; Είστε

- Πολύ ανήσυχος Αρκετά Ανήσυχος Όχι ιδιαίτερα ανήσυχος Καθόλου Ανήσυχος Δεν γνωρίζω

5. Πόσο άνετα νιώθετε με το γεγονός ότι οι ιστοσελίδες εταιρειών χρησιμοποιούν την πληροφορία για την online δραστηριότητά σας, ώστε να διαμορφώσουν περιεχόμενο που ανταποκρίνεται στις προτιμήσεις σας; (πχ. προσωποποιημένες διαφημίσεις)

- Πολύ άνετα Αρκετά Άνετα Όχι ιδιαίτερα Άνετα Καθόλου Άνετα Δεν γνωρίζω

6. Σε ποιο βαθμό σας απασχολεί το γεγονός ότι Αρχές και ιδιωτικές εταιρίες που φυλάσσουν πληροφορίες για εσάς μπορεί ορισμένες φορές να τις χρησιμοποιήσουν για διαφορετικούς λόγους από αυτούς για τους οποίους είχαν συλλεγεί αρχικά, χωρίς όμως να σας ενημερώσουν;

Πολύ Αρκετά Όχι ιδιαίτερα Καθόλου Δεν με έχει απασχολήσει το θέμα

7. Σε ποιο βαθμό σας προβληματίζει το γεγονός ότι δημοφιλείς μηχανές αναζήτησης, όπως η Google, καταγράφουν τις ιστοσελίδες από τις οποίες προήλθατε καθώς και αυτές τις οποίες επισκέπτεστε;

Πολύ Αρκετά Όχι ιδιαίτερα Καθόλου Δεν με έχει απασχολήσει το θέμα

8. Θα θέλατε να έχετε πληροφόρηση στην περίπτωση που χαθούν ή κλαπούν τα προσωπικά σας δεδομένα;

Ναι Όχι

9. Τι είδους δεδομένα θα σας απασχολούσε πιο πολύ σε περίπτωση που χαθούν ή κλαπούν; (Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις)

- Δεδομένα που είναι αποθηκευμένα στον Υπολογιστή σας
- Δεδομένα που είναι αποθηκευμένα στην κινητή σας συσκευή
- Δεδομένα που είναι αποθηκευμένα online ή σε cloud
- Άλλο
- Δεν γνωρίζω

10. Ποιοι είναι για εσάς οι πιο σοβαροί κίνδυνοι για τα προσωπικά σας δεδομένα, όταν παρέχετε προσωπικές πληροφορίες online; (Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις)

- Να πέσετε θύμα απάτης
- Η ψηφιακή σας ταυτότητα να χρησιμοποιηθεί για λόγους απάτης
- Οι πληροφορίες σας να χρησιμοποιηθούν χωρίς να το γνωρίζετε
- Να κλαπούν οι προσωπικές σας πληροφορίες
- Οι πληροφορίες σας να διανεμηθούν σε τρίτους (εταιρίες ή κρατικές υπηρεσίες) χωρίς τη συγκατάθεσή σας
- Οι πληροφορίες σας να χρησιμοποιηθούν για διαφορετικό λόγο από αυτόν που τις παρείχατε αρχικά
- Οι πληροφορίες σας να χρησιμοποιηθούν για να σας αποσταλεί ανεπιθύμητο διαφημιστικό υλικό
- Η προσωπική σας ασφάλεια να τεθεί σε κίνδυνο
- Να πληγεί η φήμη σας

- Να πέσετε θύμα διακρίσεων (πχ προσλήψεις εργασίας, να σας χρεώσουν υψηλότερες τιμές, να σας απαγορευθεί η πρόσβαση σε κάποια υπηρεσία)
- Οι απόψεις σας και η συμπεριφορά σας να παρεξηγηθούν
- Άλλο
- Κανένας κίνδυνος
- Δεν παρέχετε ποτέ προσωπικές πληροφορίες Online
- Δεν γνωρίζω

Γ.2 Προστασία Προσωπικών δεδομένων

1. *Σκεπτόμενοι τις δηλώσεις απορρήτου στο διαδίκτυο, ποια από τις παρακάτω προτάσεις περιγράφει καλύτερα αυτό που συνήθως κάνετε;*

- Τις διαβάζω ολόκληρες
- Τις διαβάζω μερικώς
- Δεν τις διαβάζω

2. *Ποιοι είναι οι λόγοι που διαβάζετε μερικώς ή και καθόλου τις δηλώσεις απορρήτου στο διαδίκτυο; (Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις)*

- Είναι πολύ μεγάλο το κείμενο για να το διαβάσω
- Δεν είναι ξεκάθαρες, είναι δυσνόητες
- Πιστεύετε ότι οι ιστότοποι δεν θα τις τηρήσουν έτσι και αλλιώς
- Πιστεύετε ότι η νομοθεσία θα σας προστατεύσει σε κάθε περίπτωση
- Σας αρκεί να βλέπετε ότι οι ιστότοποι διαθέτουν πολιτικές απορρήτου
- Δεν νομίζετε ότι είναι κάτι σημαντικό για να τις διαβάσετε
- Δεν γνωρίζετε που να τις βρείτε
- Άλλο
- Δεν γνωρίζω

3. *Σε ποιον θα απευθυνθείτε σε περίπτωση που αντιμετωπίζετε κάποιο πρόβλημα σχετικά με την προστασία των προσωπικών σας δεδομένων; (Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις)*

- Αρμόδια Ρυθμιστική Αρχή
- Αρχή ή ιδιωτικός φορέας που διαχειρίζεται τα δεδομένα σας
- Δικαστήριο
- Κάποια Ανεξάρτητη Αρχή για την προστασία του υποκειμένου των δεδομένων
- Ευρωπαϊκή Αρχή
- Άλλο
- Δεν γνωρίζω
- Δεν θα απευθυνθώ σε κανέναν

4. *Δίνετε με σαφή τρόπο τη συγκατάθεση σας προκειμένου κάθε είδος προσωπικής πληροφορίας να συλλεγεί και να επεξεργαστεί;*

- Ναι, σε κάθε περίπτωση
- Ναι, στην περίπτωση που τα δεδομένα ζητούνται online
- Ναι, στην περίπτωση που πρόκειται για ευαίσθητα προσωπικά δεδομένα
- Όχι
- Δεν είμαι βέβαιος/η

5. Όταν δίνετε προσωπικές πληροφορίες online, θα λέγατε ότι έχετε πληροφόρηση για τις συνθήκες συλλογής και επεξεργασίας των δεδομένων σας;

Πάντα Ορισμένες φορές Σπάνια Ποτέ Δεν σας έχει ζητηθεί ποτέ να δώσετε προσωπικές πληροφορίες online Δεν γνωρίζω

6. Σε περίπτωση που αποφασίσετε να αλλάξετε πάροχο online υπηρεσιών (π.χ. Online Κοινωνικό Δίκτυο, υπηρεσία cloud κλπ.), πόσο σημαντικό είναι για εσάς να έχετε την ευχέρεια να μεταφέρετε τα προσωπικά σας δεδομένα από τον παλιό πάροχο στον καινούριο;

Πολύ σημαντικό Αρκετά σημαντικό Όχι ιδιαίτερα σημαντικό Καθόλου σημαντικό Δεν γνωρίζω

7. Δηλώστε, παρακαλούμε, τη συμφωνία ή τη διαφωνία σας με τις ακόλουθες προτάσεις

α) Είμαι βέβαιος/η ότι τα προσωπικά δεδομένα που παρέχω δεν αξιοποιηθούν από κανέναν άλλο

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

β) Γνωρίζω καλά τη νομοθεσία για την προστασία των δεδομένων μου για να προστατεύσω τον εαυτό μου

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

γ) Εμπιστεύομαι τους παρόχους υπηρεσιών για να προστατεύουν τα δεδομένα μου

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

δ) Η νομοθεσία και οι ρυθμιστικές αρχές προστατεύουν πλήρως τα προσωπικά μου δεδομένα.

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

ε) Για να προστατευθώ είναι αρκετό να είμαι προσεκτικός στα δεδομένα που παρέχω online.

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

στ) Οι κυβερνήσεις προστατεύουν τα δεδομένα μου.

Συμφωνώ απόλυτα Συμφωνώ Ούτε συμφωνώ, ούτε διαφωνώ Διαφωνώ Διαφωνώ απόλυτα

Δ. Ατομικές Πληροφορίες

Φύλο

- Άνδρας Γυναίκα

Ηλικία

- 18 - 25
 26 - 35
 36 - 45
 46 - 55
 > 56

Επίπεδο Εκπαίδευσης

- Απόφοιτος/η Δημοτικού
 Απόφοιτος/η Γυμνασίου
 Απόφοιτος/η Λυκείου
 Απόφοιτος Α.Ε.Ι
 Κάτοχος μεταπτυχιακού τίτλου
 Κάτοχος διδακτορικού τίτλου

Επάγγελμα

- Δημόσιος Υπάλληλος
 Ιδιωτικός Υπάλληλος
 Ελεύθερος Επαγγελματίας
 Εκπαιδευτικός (όλες οι βαθμίδες)
 Φοιτητής/τρια
 Συνταξιούχος
 Άλλο

Σας ευχαριστούμε για τη συμμετοχή σας

Γ.1 Αποτελέσματα ενότητας ερωτηματολογίου Α. «Γενικός Κανονισμός Προστασίας Δεδομένων»

Ερώτηση Α.1

Inform_GDPR

	Frequency	Percent	Valid Percent	Cumulative Percent
Mass Media	14	13,9	13,9	13,9
Internet	45	44,6	44,6	58,4
Valid Personal interest/engagement	25	24,8	24,8	83,2
Informed by someone	17	16,8	16,8	100,0
Total	101	100,0	100,0	

Ερώτηση Α.2

GDPR_implementation_responsibility

	Frequency	Percent	Valid Percent	Cumulative Percent
European Union	83	82,2	82,2	82,2
Country	7	6,9	6,9	89,1
Valid Region	1	1,0	1,0	90,1
Don't know	10	9,9	9,9	100,0
Total	101	100,0	100,0	

Ερώτηση A.3

GDPR_responds

	Frequency	Percent	Valid Percent	Cumulative Percent
users rights enhancement	5	5,0	5,0	5,0
increase of controllers obligations	2	2,0	2,0	6,9
stricter delimitation of procedures	18	17,8	17,8	24,8
compliance with legislation	5	5,0	5,0	29,7
all	22	21,8	21,8	51,5
rights enhancement, obligations increase, stricter delimitation	7	6,9	6,9	58,4
rights enhancement, stricter delimitation	10	9,9	9,9	68,3
obligations increase, stricter delimitation	9	8,9	8,9	77,2
rights enhancement, stricter delimitation, compliance	7	6,9	6,9	84,2
Valid obligations increase, stricter delimitation, compliance	4	4,0	4,0	88,1
stricter delimitation, compliance	2	2,0	2,0	90,1
rights enhancement, obligations increase, compliance	2	2,0	2,0	92,1
rights enhancement, obligations increase	4	4,0	4,0	96,0
obligations increase, compliance	1	1,0	1,0	97,0
obligations increase, stricter delimitation,compliance	2	2,0	2,0	99,0
users rights enhancement, compliance	1	1,0	1,0	100,0
Total	101	100,0	100,0	

Ερώτηση A.4

Know_Regul_Authority_Greece

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	59	58,4	58,4	58,4
Valid No	42	41,6	41,6	100,0
Total	101	100,0	100,0	

Γ.2 Αποτελέσματα ενότητας ερωτηματολογίου Β. «Τα δικαιώματα των υποκειμένων»

Ερώτηση Β.1

Right_inform_process

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	10	9,9	10,0	10,0
Valid little	11	10,9	11,0	21,0
Valid medium	24	23,8	24,0	45,0
Valid well	29	28,7	29,0	74,0
Valid very well	26	25,7	26,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.2

Right_correct_inaccurate_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	11	10,9	11,1	11,1
Valid little	11	10,9	11,1	22,2
Valid medium	31	30,7	31,3	53,5
Valid well	27	26,7	27,3	80,8
Valid very well	19	18,8	19,2	100,0
Total	99	98,0	100,0	
Missing System	2	2,0		
Total	101	100,0		

Ερώτηση Β.3

Consensus_required_for_data_process

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	5	5,0	5,0	5,0
little	10	9,9	10,0	15,0
medium	10	9,9	10,0	25,0
well	28	27,7	28,0	53,0
very well	47	46,5	47,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.4

Consensus_specific_explicit

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	8	7,9	7,9	7,9
little	8	7,9	7,9	15,8
medium	24	23,8	23,8	39,6
well	37	36,6	36,6	76,2
very well	24	23,8	23,8	100,0
Total	101	100,0	100,0	

Ερώτηση Β.5

Consensus_recalled

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	19	18,8	19,4	19,4
little	12	11,9	12,2	31,6
medium	22	21,8	22,4	54,1
well	18	17,8	18,4	72,4
very well	27	26,7	27,6	100,0
Total	98	97,0	100,0	
Missing System	3	3,0		
Total	101	100,0		

Ερώτηση Β.6

Consensus_not_required_for_service_usage

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	17	16,8	17,0	17,0
Valid little	17	16,8	17,0	34,0
Valid medium	29	28,7	29,0	63,0
Valid well	21	20,8	21,0	84,0
Valid very well	16	15,8	16,0	100,0
Valid Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.7

Right_inform_profiling

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	15	14,9	15,0	15,0
Valid little	20	19,8	20,0	35,0
Valid medium	20	19,8	20,0	55,0
Valid well	30	29,7	30,0	85,0
Valid very well	15	14,9	15,0	100,0
Valid Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.8

Right_inform_data_transmission

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	19	18,8	19,0	19,0
Valid little	20	19,8	20,0	39,0
Valid medium	18	17,8	18,0	57,0
Valid well	21	20,8	21,0	78,0
Valid very well	22	21,8	22,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.9

Right_inform_data_breach

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	19	18,8	18,8	18,8
Valid little	21	20,8	20,8	39,6
Valid medium	20	19,8	19,8	59,4
Valid well	19	18,8	18,8	78,2
Valid very well	22	21,8	21,8	100,0
Total	101	100,0	100,0	

Ερώτηση Β.10

Right_oppose_data_process

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	14	13,9	14,0	14,0
Valid little	26	25,7	26,0	40,0
Valid medium	22	21,8	22,0	62,0
Valid well	24	23,8	24,0	86,0
Valid very well	14	13,9	14,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.11

Right_not_subject_automated_desicion

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	18	17,8	18,0	18,0
Valid little	29	28,7	29,0	47,0
Valid medium	26	25,7	26,0	73,0
Valid well	16	15,8	16,0	89,0
Valid very well	11	10,9	11,0	100,0
Valid Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Β.12

Right_transport_data_other_processor

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid not at all	30	29,7	30,0	30,0
Valid little	24	23,8	24,0	54,0
Valid medium	15	14,9	15,0	69,0
Valid well	23	22,8	23,0	92,0
Valid very well	8	7,9	8,0	100,0
Valid Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση B.13

Right_delete_personal_data_if

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid data no longer necessary	6	5,9	5,9	5,9
consensus withdraw	22	21,8	21,8	27,7
no legal base for processing	2	2,0	2,0	29,7
don't know	23	22,8	22,8	52,5
all cases	15	14,9	14,9	67,3
consensus withdraw, no legal base	13	12,9	12,9	80,2
data no longer necessary, consensus withdraw	15	14,9	14,9	95,0
data no longer necessary, no legal base	5	5,0	5,0	100,0
Total	101	100,0	100,0	

Statistics

	Data_no_longer_necessary	consensus_withdraw	no_legal_base_processing	dont_know
N Valid	41	65	35	23
Mode	1,00	1,00	1,00	1,00

Ερώτηση B.14

Right_restriction_data_processing_if

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid data accuracy questioned	2	2,0	2,0	2,0
illegal processing	8	7,9	7,9	9,9
data no longer required for processing	2	2,0	2,0	11,9
objections to processing	7	6,9	6,9	18,8
don't know	30	29,7	29,7	48,5
all cases	10	9,9	9,9	58,4
illegal processing, data no longer required	2	2,0	2,0	60,4

illegal processing, data no longer required, objections to processing	8	7,9	7,9	68,3
data accuracy, illegal processing, objections	7	6,9	6,9	75,2
data no longer required, objections	6	5,9	5,9	81,2
data accuracy, data no longer required	2	2,0	2,0	83,2
data accuracy, data no longer required, objections	2	2,0	2,0	85,1
data accuracy, objections	2	2,0	2,0	87,1
data accuracy, illegal processing	4	4,0	4,0	91,1
illegal processing, objections	7	6,9	6,9	98,0
data accuracy, illegal processing, data no longer required	2	2,0	2,0	100,0
Total	101	100,0	100,0	

Statistics

	Data_accuracy	Illegal_processing	Data_no_longer_required	Objections	Do_not_know
N Valid	31	48	34	49	30
Mode	1,00	1,00	1,00	1,00	1,00

Γ.3 Αποτελέσματα υποενότητας ερωτηματολογίου Γ.1 «Έλεγχος προσωπικών δεδομένων και κίνδυνοι»

Ερώτηση Γ.1.1

Control_data_given_online

	Frequency	Percent	Valid Percent	Cumulative Percent
not sure at all	14	13,9	13,9	13,9
not really sure	34	33,7	33,7	47,5
Valid pretty sure	40	39,6	39,6	87,1
absolutely sure	13	12,9	12,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.2

Feel_control_data_online

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Don't Know	5	5,0	5,0	5,0
Depends	16	15,8	16,0	21,0
No control	20	19,8	20,0	41,0
Partial control	56	55,4	56,0	97,0
Full control	3	3,0	3,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Γ.1.3

Feel_worried_other_control_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Don't Know	1	1,0	1,0	1,0
Not at all worried	2	2,0	2,0	3,0
No particularly worried	15	14,9	14,9	17,8
Quite worried	68	67,3	67,3	85,1
Very worried	15	14,9	14,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.4

Feel_worried_governments_collect_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Don't Know	1	1,0	1,0	1,0
Not at all worried	5	5,0	5,0	6,0
No particularly worried	23	22,8	23,0	29,0
Quite worried	49	48,5	49,0	78,0
Very worried	22	21,8	22,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Γ.1.5

Feel_comfortable_websites_use_personal_information

	Frequency	Percent	Valid Percent	Cumulative Percent
Very comfortable	1	1,0	1,0	1,0
Quite comfortable	10	9,9	9,9	10,9
No particularly comfortable	41	40,6	40,6	51,5
Not at all comfortable	49	48,5	48,5	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.6

Fell_worried_data_usage_different_reason

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Have not thought the issue	1	1,0	1,0	1,0
Not at all worried	3	3,0	3,0	4,0
No particularly worried	7	6,9	6,9	10,9
Quite worried	50	49,5	49,5	60,4
Very worried	40	39,6	39,6	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.7

Feel_worried_search_engines_record_websites

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Have not thought the issue	3	3,0	3,0	3,0
Not at all worried	4	4,0	4,0	6,9
No particularly worried	10	9,9	9,9	16,8
Quite worried	56	55,4	55,4	72,3
Very worried	28	27,7	27,7	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.9

Data_loss_stealen

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid stored in PC	11	10,9	10,9	10,9
stored in mobile device	8	7,9	7,9	18,8
stored online/cloud	4	4,0	4,0	22,8
all cases	52	51,5	51,5	74,3
stored in PC, stored in mobile device	21	20,8	20,8	95,0
stored in PC, stored online/cloud	3	3,0	3,0	98,0
stored in mobile device, stored online/cloud	2	2,0	2,0	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.1.10

Statistics

	Risks_fraud_victim	Risks_digital_identity_used_fraud	Risks_data_used_without_knowing	Risks_personal_information_stolen	Risks_personal_information_distributed_others	Risks_personal_information_usage_different_reason
N Valid	77	78	64	66	65	58

Statistics

	Risks_personal_information_usage_personalized_content	Risks_personal_security_damage	Risks_reputation_damage	Risks_discrimination_victim	Risks_views_behavior_misunderstood	Risks_Other
N Valid	35	75	56	48	38	4

Γ.4 Αποτελέσματα υποεπάρκειας ερωτηματολογίου Γ.2 «Προστασία προσωπικών δεδομένων»

Ερώτηση Γ.2.1

Read_privacy_statements

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Don't read	29	28,7	28,7	28,7
Valid Read partially	65	64,4	64,4	93,1
Valid Read whole text	7	6,9	6,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.2

Statistics

	Reason_long_t ext	Reason_not_cle ar	Reason_not_ap plied_websites	Reason_law_pr otection
N Valid	75	56	22	9
Mode	1,00	1,00	1,00	1,00

Statistics

	Reason_websit es_privacy_poli cy	Reason_not_im portant	Reason_not_kn ow_find	Reason_other
N Valid	14	4	2	3
Mode	1,00	1,00	1,00	1,00

Ερώτηση Γ.2.3

Whom_address_data_protection

	Frequency	Percent	Valid Percent	Cumulative Percent
Regulatory Authority	29	28,7	28,7	28,7
Authority or private entity managing my data	6	5,9	5,9	34,7
Court	4	4,0	4,0	38,6
Independent Authority for the protection of the data	11	10,9	10,9	49,5
European Authority	2	2,0	2,0	51,5
Other	1	1,0	1,0	52,5
Don't know	12	11,9	11,9	64,4
No one	1	1,0	1,0	65,3
Regul.Authority, authority or entity	16	15,8	15,8	81,2
Regul.Authority, independent authority	3	3,0	3,0	84,2
Regul.Authority, court	3	3,0	3,0	87,1
Regul.Authority, authority or entity, Independent authority	2	2,0	2,0	89,1
authority or entity, independent authority	2	2,0	2,0	91,1

Regul.Authority, authority or entity, European authority	2	2,0	2,0	93,1
Regul.Authority, authority or entity, court, european authority	1	1,0	1,0	94,1
Regul.Authority, authority or entity, Independent authority, European authority	1	1,0	1,0	95,0
Regul.Authority, court, Independent authority, European authority	1	1,0	1,0	96,0
Authority or private entity, European Authority	1	1,0	1,0	97,0
Regul. Authority, Authority or private entity	2	2,0	2,0	99,0
Regul.Authority, court, independent authority	1	1,0	1,0	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.4

Consensus_data_process

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Yes, in any case	19	18,8	19,0	19,0
Yes, in the case of online data	19	18,8	19,0	38,0
Yes, in the case of sensitive data	16	15,8	16,0	54,0
No	21	20,8	21,0	75,0
Not sure	25	24,8	25,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Γ.2.5

Informed_conditions_collection_processing_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Always	4	4,0	4,0	4,0
Sometimes	38	37,6	37,6	41,6
Rarely	40	39,6	39,6	81,2
Never	11	10,9	10,9	92,1
Valid Have not been asked to give infor. online	2	2,0	2,0	94,1
Don't know	6	5,9	5,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.6

Importance_data_transport_other_provider

	Frequency	Percent	Valid Percent	Cumulative Percent
Don't know	4	4,0	4,0	4,0
Not important at all	2	2,0	2,0	5,9
Valid No particularly important	19	18,8	18,8	24,8
Quite important	37	36,6	36,6	61,4
Very important	39	38,6	38,6	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.α

Sure_personal_data_not_used_anyone

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	3	3,0	3,0	3,0
Agree	15	14,9	14,9	17,8
Valid Neither agree, nor disagree	29	28,7	28,7	46,5
Disagree	35	34,7	34,7	81,2
Totally disagree	19	18,8	18,8	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.β

Know_law_well_protect_myself

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	1	1,0	1,0	1,0
Agree	26	25,7	25,7	26,7
Neither agree, nor disagree	35	34,7	34,7	61,4
Disagree	25	24,8	24,8	86,1
Totally disagree	14	13,9	13,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.γ

Trust_providers_protect_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	2	2,0	2,0	2,0
Agree	15	14,9	14,9	16,8
Neither agree, nor disagree	31	30,7	30,7	47,5
Disagree	37	36,6	36,6	84,2
Totally disagree	16	15,8	15,8	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.δ

Law_RegAuthorities_protect_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	3	3,0	3,0	3,0
Agree	17	16,8	16,8	19,8
Neither agree, nor disagree	40	39,6	39,6	59,4
Disagree	36	35,6	35,6	95,0
Totally disagree	5	5,0	5,0	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.ε

To_protect_carefull_data_reveal

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	10	9,9	9,9	9,9
Agree	23	22,8	22,8	32,7
Neither agree, nor disagree	33	32,7	32,7	65,3
Disagree	26	25,7	25,7	91,1
Totally disagree	9	8,9	8,9	100,0
Total	101	100,0	100,0	

Ερώτηση Γ.2.7.στ

Governments_protect_data

	Frequency	Percent	Valid Percent	Cumulative Percent
Totally agree	3	3,0	3,0	3,0
Agree	11	10,9	10,9	13,9
Neither agree, nor disagree	25	24,8	24,8	38,6
Disagree	43	42,6	42,6	81,2
Totally disagree	19	18,8	18,8	100,0
Total	101	100,0	100,0	

Γ.5 Αποτελέσματα ενότητας ερωτηματολογίου Δ.
«Ατομικές Πληροφορίες»

Ερώτηση Δ.1

Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Man	49	48,5	49,0	49,0
Valid Woman	51	50,5	51,0	100,0
Total	100	99,0	100,0	
Missing System	1	1,0		
Total	101	100,0		

Ερώτηση Δ.2

Age

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 18-25	6	5,9	5,9	5,9
26-35	26	25,7	25,7	31,7
36-45	50	49,5	49,5	81,2
46-55	16	15,8	15,8	97,0
>56	3	3,0	3,0	100,0
Total	101	100,0	100,0	

Ερώτηση Δ.3

Education_level

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid graduate_secondary education_high school	16	15,8	15,8	15,8
graduate_university	39	38,6	38,6	54,5
M.Sc.	43	42,6	42,6	97,0
Ph.D	3	3,0	3,0	100,0
Total	101	100,0	100,0	

Ερώτηση Δ.4

Employment

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid employee_public sector	37	36,6	36,6	36,6
employee_private sector	32	31,7	31,7	68,3
Freelancer	18	17,8	17,8	86,1
Teacher	2	2,0	2,0	88,1
Student	9	8,9	8,9	97,0
Other	3	3,0	3,0	100,0
Total	101	100,0	100,0	