Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Προστασία των Δεδομένων Προσωπικού Χαρακτήρα στον Τομέα της Ηλεκτρονικής Υγείας

Μαρία Καραγεώργου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Προστασία των Δεδομένων Προσωπικού Χαρακτήρα στον Τομέα της Ηλεκτρονικής Υγείας

Μαρία Καραγεώργου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2018

Περίληψη

Οι τεχνολογικές εξελίξεις των τελευταίων ετών, στο υλικό (hardware) των «έξυπνων» συσκευών, όπως smartphones και tablets, καθώς και η πρόοδος στις τηλεπικοινωνίες έχουν σαν αποτέλεσμα την ανάπτυξη - χαμηλού κόστους – κινητών συσκευών, οι οποίες πλέον είναι προσιτές σχεδόν από όλους. Κατά συνέπεια, νέες λειτουργίες-υπηρεσίες, οι οποίες βασίζονται στις εξελίξεις αυτές, επιτρέπουν σε εκατομμύρια εφαρμογών (applications) να αξιοποιούν-εκμεταλλεύονται τεράστιες ποσότητες δεδομένων. Οι εφαρμογές mobile health (m-health) δεν θα μπορούσαν παρά να ακολουθήσουν την τάση αυτή. Έτσι, οι εν λόγω εφαρμογές συγκεντρώνουν – σχετικές με την υγεία των χρηστών – πληροφορίες, προκειμένου να προωθήσουν το «ευ ζην» αυτών. Παρ' όλα αυτά, οι πληροφορίες που σχετίζονται με την υγεία αποτελούν Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα. Επομένως, η προστασία τους έχει ιδιάζουσα σημασία.

Αντικείμενο της παρούσας μεταπτυχιακής διατριβής είναι η αποτίμηση του βαθμού προστασίας των Δεδομένων Προσωπικού Χαρακτήρα στον τομέα της Ηλεκτρονικής Υγείας και ιδιαίτερα στην περίπτωση των «έξυπνων» εφαρμογών. Στην αρχή παρουσιάζεται το ισχύον νομοθετικό πλαίσιο για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα τόσο σε εθνικό, όσο και σε επίπεδο Ευρωπαϊκής Ένωσης, καθώς και ένα σύντομο ιστορικό για το πώς φτάσαμε σε αυτό (Γενικός Κανονισμός Προστασίας Δεδομένων - GDPR). Στην συνέχεια παρουσιάζονται κάποιες ενδεικτικές εφαρμογές m-health αναλύοντας τις πληροφορίες που ζητούνται από τον χρήστη κατά την εγκατάσταση, οι Όροι Χρήσης, καθώς και η Πολιτική Ασφάλειας της καθεμιάς, υπό το πρίσμα του κατά πόσον η επεξεργασία των ευαίσθητων προσωπικών δεδομένων που πραγματοποιούν αυτές είναι οι εφαρμογές είναι σύμφωνη με τις νομικές επιταγές για την προστασία προσωπικών δεδομένων.

Τα αποτελέσματα της ανάλυσης των m-health εφαρμογών αποδεικνύουν ότι οι δημιουργοί των εφαρμογών αυτών (σχεδιαστές, προγραμματιστές, αναλυτές, κτλ) δεν δίνουν την πρέπουσα σημασία στην προστασία των Δεδομένων Προσωπικού Χαρακτήρα. Ακόμη και σε επίπεδο μελετών δίνεται μεγαλύτερη βαρύτητα στον τομέα της Ασφάλειας, ενώ οι τομείς της Ιδιωτικότητας και της Προστασίας των Δεδομένων έχουν δευτερεύοντα ρόλο.

Λέξεις – Κλειδιά: Προσωπικά δεδομένα, ηλεκτρονική υγεία, λειτουργικό σύστημα android, m-health εφαρμογές, γενικός κανονισμός προστασίας δεδομένων (GDPR), όροι χρήσης, πολιτική ασφάλειας

Summary

The technological evolution of recent years in hardware of smart devices, such as smartphones and tablets, as well as the progress in telecommunications have resulted the development of low cost mobile devices, which are now accessible almost to everyone. Consequently, new functionalities, based on these developments, allow millions of applications to use-take advantage of immense amounts of data. M-health applications could only follow this trend. Thus, these applications bring together - related to the health of users - information in order to promote their "well-being". Nonetheless, health-related information is Sensitive Personal Data. Their protection is therefore of particular importance.

The purpose of this postgraduate dissertation is to evaluate the degree of protection of Personal Data in the field of e-Health and especially in the case of "smart" applications. In the beginning, we will present the current legislative framework for the protection of Personal Data at both national and EU level, as well as a brief history of how we have reached it (General Data Protection Regulation - GDPR). Moreover, some m-health indicative applications are studied in terms of analyzing the information requested by the user during the installation, the Terms of Use, and the Security Policy of each will be analyzed. Such analysis focuses on determining whether the personal data processing that is taking place is in compliance with the corresponding data protection legislation.

The results of the analysis of m-health applications show that the creators of these applications (designers, developers, analysts, etc.) do not attach sufficient importance to the protection of Personal Data. Even in the field of studies, greater emphasis is placed on security, while the areas of Privacy and Data Protection have a secondary role.

Key Words:

Personal data, e-health, android operating system, m-health applications, general data protection regulation (GDPR), terms of use, security policy

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου Δρ. Κωνσταντίνο Λιμνιώτη για την εμπιστοσύνη που έδειξε στο πρόσωπό μου με την ανάθεση αυτής της μεταπτυχιακής διατριβής. Η άριστη καθοδήγησή του, η παροιμιώδης επιμονή του, καθώς και η απεριόριστη κατανόησή του, συνέβαλαν καθοριστικά στην επιτυχή ολοκλήρωση της διατριβής αυτής.

Επίσης, ευχαριστώ θερμά την οικογένειά μου, τους συναδέλφους μου και τους φίλους μου για την κατανόησή τους και την αμέριστη συμπαράστασή τους όχι μόνο κατά το διάστημα εκπόνησης της παρούσας διατριβής, αλλά και καθ' όλη την διάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Πλησιάζουμε στο τέλος της δεύτερης δεκαετίας του 21ου αιώνα και ταυτόχρονα γινόμαστε μάρτυρες μιας αλματώδους εξέλιξης της τεχνολογίας. Πλέον, δεν κάνουμε λόγο για εισβολή των νέων τεχνολογιών στον ανεπτυγμένο κόσμο, αλλά για πλήρη επικράτησή τους. Η γρήγορη διάδοση της ασύρματης σύνδεσης στο διαδίκτυο, σε συνδυασμό με την ταχύτατη ανάπτυξη στον τομέα των τηλεπικοινωνιών, έχουν ως αποτέλεσμα την καθημερινή μας πρόσβαση σε όγκο και ποικιλία πληροφοριών που – μόλις μια δεκαετία πριν - ούτε καν είχαμε φανταστεί.

Αποκύημα αυτής της ραγδαίας τεχνολογικής εξέλιξης είναι η κατασκευή συσκευών όπως τα «έξυπνα» κινητά τηλέφωνα, γνωστά σαν smartphones, και τα tablets. Για τη αξιοποίησή τους έχουν αναπτυχθεί αντίστοιχα λειτουργικά συστήματα όπως το Android και το iPhone OS, με τα οποία μπορούν οι χρήστες να εγκαταστήσουν πληθώρα εφαρμογών που τους προσφέρουν ψυχαγωγία, ενημέρωση, επικοινωνία, κτλ. Οι συσκευές αυτές έτυχαν καθολικής αποδοχής από τους χρήστες, λόγω των συγκριτικών τους πλεονεκτημάτων και είχαν σαν αποτέλεσμα την ριζική αλλαγή στον τρόπο που χρησιμοποιούμε τις κινητές συσκευές και τις πληροφορίες που ανταλλάσουμε μέσω αυτών. Η αλλαγή αυτή ενισχύθηκε, εν μέρει, από την ύπαρξη πολλών

ενσωματωμένων αισθητήρων, που χρησιμοποιούν οι προγραμματιστές για να παρέχουν στις εφαρμογές τους επιπλέον δυνατότητες.

Έτσι, ο τομέας των mobile applications (apps) έφτασε σήμερα να θεωρείται μία από τις μεγαλύτερες βιομηχανίες παγκοσμίως, η οποία περιλαμβάνει εκατομμύρια προγραμματιστών εφαρμογών και δισεκατομμύρια ιδιοκτητών smartphones, οι οποίοι χρησιμοποιούν τις εφαρμογές των κινητών τους σε καθημερινή βάση. Πρόσφατες στατιστικές αναφέρουν ότι για το 2017 οι λήψεις mobile apps ξεπέρασαν τα 197 δις, με πιο δημοφιλείς κατηγορίες αυτές των παιχνιδιών, της διασκέδασης, της ενημέρωσης, της κοινωνικής δικτύωσης, της υγείας-υγιεινής ζωής, κτλ.

Ωστόσο, τη στιγμή που οι συνδεδεμένοι χρήστες βασίζονται όλο και περισσότερο στις «έξυπνες» φορητές συσκευές τους (π.χ. smartphones και tablets) για τις καθημερινές τους δραστηριότητες και ανάγκες, η επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα από τις συσκευές αυτές δεν είναι πάντοτε διαφανής ή ελεγχόμενη από τους χρήστες. Επιπλέον, η κατανόηση από τους χρήστες του τρόπου λειτουργίας των εφαρμογών αυτών είναι μία δύσκολη υπόθεση, μιας και αναπτύσσονται σε ένα δυναμικό περιβάλλον, επαναχρησιμοποιούν βιβλιοθήκες λογισμικού και διασυνδέονται με ποικίλα δίκτυα και συστήματα. Όλα αυτά καθιστούν την εκτίμηση των χαρακτηριστικών τους – σε σχέση με την ιδιωτικότητα και την ασφάλεια – σχεδόν ακατόρθωτη για τον μέσο χρήστη. Παρ' όλο που ελάχιστοι προγραμματιστές εφαρμογών θα παρέβλεπαν τις υποχρεώσεις τους για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα από κακή πρόθεση, σε πολλές περιπτώσεις το χαμηλό επίπεδο της προστασίας των δεδομένων, αλλά και της ασφάλειας εν γένει, οφείλεται σε έλλειψη γνώσης ή κατανόησης των κινδύνων ή ακόμη και σε άγνοια των πρακτικών προστασίας των εφαρμογών τους, αλλά και του συναφούς νομικού πλαισίου.

Η επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα στις εφαρμογές θα ρυθμίζεται πλέον από τον Γενικό Κανονισμό Προστασίας Δεδομένων - ΓΚΠΔ (General Data Protection Regulation – GDPR) [54], ο οποίος θα είναι – από τις 25 Μαΐου 2018 – το κύριο νομικό πλαίσιο για την προστασία των δεδομένων στην Ευρωπαϊκή ένωση, με άμεση ισχύ σε όλα τα κράτη-μέλη, αντικαθιστώντας την έως τώρα ισχύουσα οδηγία 95/46/ΕΚ [62], η οποία είχε ενσωματωθεί στην έννομη τάξη κάθε Κράτους-Μέλους. Ενώ ενισχύει τις αρχές, τις υποχρεώσεις και τα δικαιώματα περί προστασίας δεδομένων, τα οποία είχαν κατοχυρωθεί στην οδηγία, ο ΓΚΠΔ περιλαμβάνει επιπλέον μηχανισμούς προστασίας, προκειμένου να επιτρέψει στους χρήστες τον

καλύτερο έλεγχο των Δεδομένων Προσωπικού Χαρακτήρα. Αυτό αποτελεί μία ιδιαίτερη πρόκληση όταν πρόκειται για ένα κινητό online περιβάλλον.

Στις διατάξεις του ΓΚΠΔ για την Ιδιωτικότητα στις mobile εφαρμογές και τις απαιτήσεις για την προστασία των δεδομένων, συνεπικουρεί και η οδηγία 2002/58/ΕΚ [60] για την Ιδιωτικότητα στις ηλεκτρονικές επικοινωνίες, η οποία βρίσκεται - και αυτή - υπό αναθεώρηση, προκειμένου να ενημερωθεί και να ευθυγραμμιστεί με τον ΓΚΠΔ. Τον Ιανουάριο του 2017 έγινε μία πρόταση για σύνταξη νέου κανονισμού για την e-Ιδιωτικότητα (ePrivacy) από την Ευρωπαϊκή Επιτροπή και – προς το παρόν - βρίσκεται για διαβούλευση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο. Αυτή η πρόταση περιέχει σημαντικές διατάξεις για την Ιδιωτικότητα και την προστασία των δεδομένων στις mobile εφαρμογές, δίνοντας ιδιαίτερη βαρύτητα στην εμπιστευτικότητα των επικοινωνιών και τα σχετικά μεταδεδομένα (metadata), την εγκατάσταση λογισμικού και δεδομένων (π.χ. cookies) στις συσκευές των χρηστών και την προστασία της ιδιωτικότητας σε σχέση με τον εντοπισμό (tracking).

Η παρούσα μεταπτυχιακή διατριβή μελετά τον βαθμό προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα της Ηλεκτρονικής Υγείας και ιδιαίτερα στην περίπτωση των «έξυπνων» εφαρμογών (m-health applications). Θα παρουσιαστούν κάποιες ενδεικτικές εφαρμογές m-health και θα αναλυθούν οι πληροφορίες που ζητούνται από τον χρήστη κατά την εγκατάσταση, οι Όροι Χρήσης, καθώς και η Πολιτική Ασφάλειας της καθεμιάς, με απώτερο στόχο να απαντηθούν τα ακόλουθα ερευνητικά ερωτήματα:

H1: Είναι η επεξεργασία προσωπικών δεδομένων σύμφωνη με τις βασικές προϋποθέσεις νομιμότητας του ΓΚΠΔ (σαφήνεια σκοπού επεξεργασίας, αναλογικότητα επεξεργασίας, λήψη συγκατάθεσης);

H2: Ικανοποιούνται τα δικαιώματα των χρηστών που προβλέπονται στον ΓΚΠΔ;

H3: Είναι η επεξεργασία των δεδομένων ασφαλής;

1.1 Δομή της Μεταπτυχιακής Διατριβής

Όπως αναφέρθηκε προηγουμένως, αντικείμενο της παρούσας μεταπτυχιακής διατριβής είναι η αποτίμηση του βαθμού προστασίας των Δεδομένων Προσωπικού Χαρακτήρα στον τομέα της

Ηλεκτρονικής Υγείας και ειδικότερα στην περίπτωση των «έξυπνων» εφαρμογών. Πιο αναλυτικά, η δομή της συγκεκριμένης διατριβής είναι η εξής:

Το κεφάλαιο 2 πραγματοποιεί μία σύντομη ιστορική αναδρομή στην ευρωπαϊκή και ελληνική νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα. Στόχος του κεφαλαίου αυτού είναι να εκθέσει τις σχετικές νομοθετικές πράξεις κατά χρονική εξέλιξη, ξεκινώντας από την παλαιότερη και καταλήγοντας στην πιο πρόσφατη. Έτσι, μπορεί να αποτελέσει μία πηγή πληροφόρησης για τον κάθε ενδιαφερόμενο, ο οποίος θα έχει την δυνατότητα να εντοπίσει, στο παρόν κείμενο, συγκεντρωμένη όλη αυτή την πληροφορία.

Το κεφάλαιο 3 κάνει μία εκτενή αναφορά στον Γενικό Κανονισμό για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα - ΓΚΠΔ (General Data Protection Regulation - GDPR) της Ευρωπαϊκής Ένωσης, ο οποίος ψηφίστηκε σχετικά πρόσφατα (Μάιος 2016). Η εφαρμογή του είναι δεσμευτική για όλα τα Κράτη-Μέλη της ΕΕ, δίνοντάς τους ένα περιθώριο δύο ετών (μέχρι τον Μάιο του 2018) για να τον ενσωματώσουν στην εθνική τους νομοθεσία. Η χρονική συγκυρία λοιπόν είναι πολύ σημαντική και γι' αυτό αφιερώνεται το συγκεκριμένο κεφάλαιο στην παρουσίαση των κυριότερων σημείων του - εν λόγω - κανονισμού.

Το κεφάλαιο 4 αναλύει το ζήτημα της προστασίας των Δεδομένων Προσωπικού Χαρακτήρα στον τομέα της Ηλεκτρονικής Υγείας. Πιο συγκεκριμένα, εξετάζει την περίπτωση των «έξυπνων» εφαρμογών στην Ηλεκτρονική Υγεία, δίνοντας έμφαση στις εφαρμογές mobile health (m-health applications) και το πώς αυτές διαχειρίζονται τα Δεδομένα Προσωπικού Χαρακτήρα των χρηστών. Επιπλέον, εδώ τίθενται τα ερευνητικά ερωτήματα της παρούσης μεταπτυχιακής διατριβής.

Το κεφάλαιο 5 περιγράφει την ανάλυση που πραγματοποιήθηκε σε συγκεκριμένες εφαρμογές m-health, προκειμένου να αποτιμηθεί ο βαθμός διασφάλισης των Δεδομένων Προσωπικού Χαρακτήρα στις εφαρμογές αυτές. Στο κεφάλαιο αυτό αποτυπώνονται τα κριτήρια με βάση τα οποία έγινε η ανάλυση των m-health εφαρμογών, καθώς και η μεθοδολογία που ακολουθήθηκε για την ανάλυση των επιλεχθέντων εφαρμογών.

Το κεφάλαιο 6 παρουσιάζει τα αποτελέσματα που προέκυψαν από την ανάλυση των m-health εφαρμογών. Επίσης, γίνεται σχολιασμός των αποτελεσμάτων, εξαγωγή των συμπερασμάτων και εντοπισμός των σημείων εκείνων που απαντούν στα ερευνητικά ερωτήματα που τέθηκαν.

Τέλος, το κεφάλαιο 7 αποτελεί τον επίλογο της παρούσας μεταπτυχιακής διατριβής και γίνεται αναφορά σε πιθανή μελλοντική έρευνα-μελέτη.

Κεφάλαιο 2

Ιστορική Αναδρομή – Η εξέλιξη της Τεχνολογίας Υπό το Πρίσμα της Νομοθεσίας

Στο παρόν κεφάλαιο θα γίνει μία παρουσίαση της – σχετικής με την προστασία των δεδομένων προσωπικού χαρακτήρα – νομοθεσίας τόσο σε εθνικό, όσο και σε επίπεδο Ευρωπαϊκής Ένωσης. Πιο συγκεκριμένα, θα γίνει μία ιστορική αναδρομή που θα παρουσιάσει το σκεπτικό της εκάστοτε ισχύουσας νομοθεσίας περί προστασίας των δεδομένων προσωπικού χαρακτήρα, με γνώμονα την αντίστοιχη εξέλιξη της τεχνολογίας στην Ευρωπαϊκή ένωση, αλλά και στην Ελλάδα.

Με λίγα λόγια, η αλματώδης εξέλιξη της τεχνολογίας τις τελευταίες δεκαετίες έχει σαν αποτέλεσμα την – χωρίς υπερβολή – εισβολή των νέων τεχνολογιών (π.χ. ασύρματες επικοινωνίες, cloud computing, Internet of Things, κτλ) σχεδόν σε κάθε πτυχή της καθημερινότητας του ανθρώπου, όπως: Επικοινωνία, υγεία, εκπαίδευση, εργασία, εμπόριο, κοκ.

Αυτό έχει σαν συνέπεια έναν τεράστιο όγκο δεδομένων προσωπικού χαρακτήρα που «ταξιδεύει» στο διαδίκτυο σε καθημερινή βάση, γεγονός που καθιστά την προστασία των δεδομένων αυτών πολύ δύσκολη υπόθεση. Για τον λόγο αυτό προκύπτει η ανάγκη διαρκούς εξέλιξης και προσαρμογής της αντίστοιχης νομοθεσίας, η οποία θα πρέπει να ανταποκρίνεται στα ζητήματα που προκύπτουν κάθε φορά από τις τεχνολογικές καινοτομίες.

2.1 Ευρωπαϊκή Ένωση

Η Ευρωπαϊκή Ένωση ή ΕΕ είναι μια ιδιότυπη υπερεθνική και διακυβερνητική ένωση 28 κρατών [52]. Καθιερώθηκε το 1993 από τη Συνθήκη για την Ευρωπαϊκή Ένωση (Συνθήκη του Μάαστριχτ), και είναι ο de facto διάδοχος των Ευρωπαϊκών Κοινοτήτων (ΕΚΑΧ, ΕΟΚ, ΕΥΡΑΤΟΜ)

των έξι Κρατών-Μελών (Βέλγιο, Δυτική Γερμανία, Γαλλία, Ιταλία, Λουξεμβούργο, Ολλανδία) που ιδρύθηκαν το 1951, το 1957 και το 1967.

Από τότε, νέες διευρύνσεις έχουν αυξήσει τον αριθμό των κρατών μελών της και οι αρμοδιότητές της έχουν επεκταθεί. Συγκεκριμένα, η Ελλάδα εισήλθε – ως πλήρες μέλος - στην τότε Ευρωπαϊκή Οικονομική Κοινότητα (ΕΟΚ) την 1η Ιανουαρίου 1981[64]. Μερικά χρόνια αργότερα (1990), και η Κύπρος θα ξεκινήσει τις αντίστοιχες ενταξιακές διαπραγματεύσεις, με αποκορύφωμα την πλήρη ένταξή της στην ΕΕ, την 1η Μαΐου 2004 [55]. Έκτοτε, και οι δύο χώρες του ελληνόφωνου κόσμου λαμβάνουν μέρος σε όλα τα θεσμικά όργανα της ΕΕ, συμμετέχουν στην λήψη των αποφάσεων και προσαρμόζουν το νομοθετικό τους πλαίσιο σύμφωνα με τις αποφάσεις αυτές [21].

2.1.1 Συνθήκη για την Ευρωπαϊκή Ένωση

Η Συνθήκη για την Ευρωπαϊκή Ένωση [63] υπογράφηκε στις 7 Φεβρουαρίου 1992, στο Μάαστριχτ της Ολλανδίας και αποτελεί στην ουσία την συνθήκη ίδρυσής της. Στο άρθρο 6, παράγραφος 2 γίνεται αναφορά στα θεμελιώδη δικαιώματα ως εξής: «Η ένωση σέβεται τα θεμελιώδη δικαιώματα, όπως κατοχυρώνονται με την Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών…». Αυτή είναι η πρώτη αναφορά για τα Δικαιώματα του Ανθρώπου και τις Θεμελιώδεις Ελευθερίες στα πλαίσια της ΕΕ. Το γεγονός ότι υπάρχει η αναφορά αυτή στην Ιδρυτική Συνθήκη της ΕΕ δείχνει και την σημασία που αποδίδουν τα Κράτη-Μέλη της ΕΕ στην προστασία αυτών.

2.1.2 Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου

Την Ιδρυτική Συνθήκη της ΕΕ που αναφέραμε παραπάνω ακολούθησε η σύνταξη της Ευρωπαϊκής Σύμβασης των δικαιωμάτων του Ανθρώπου [51], κατά τα πρότυπα της Ευρωπαϊκής Σύμβασης για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, που είχε υπογραφεί στη Ρώμη στις 4 Νοεμβρίου 1950.

Στην σύμβαση αυτή, το άρθρο 8 φέρει τον τίτλο: «Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής» και επί λέξει αναφέρει:

«*1. Παν πρόσωπον δικαιούται εις τον σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*

2. Δεν επιτρέπεται να υπάρξει επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατική κοινωνία, είναι αναγκαίον διά την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερία της χώρας, την προάσπισην της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων».

Αυτό λοιπόν που στην Συνθήκη για την Ευρωπαϊκή Ένωση ήταν μία γενική αναφορά στην ανάγκη προστασία των ανθρώπινων δικαιωμάτων και ελευθεριών, εδώ γίνεται πιο συγκεκριμένο. Μπορούμε να πούμε ότι εδώ ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας, οριοθετείται ως Θεμελιώδες Δικαίωμα του Ανθρώπου στην ΕΕ.

2.1.3 Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης [65], καθιερώνει στη νομοθεσία της ΕΕ μία σειρά προσωπικών, αστικών, πολιτικών, οικονομικών και κοινωνικών δικαιωμάτων των πολιτών και μόνιμων κατοίκων της ΕΕ. Οι άξονες της κατοχύρωσης των δικαιωμάτων αυτών είναι η Αρχή της Επικουρικότητας και η Αρχή της Αναλογικότητας [21]. Στόχος της Αρχής της Επικουρικότητας είναι να εξασφαλίζει ότι οι αποφάσεις λαμβάνονται όσο το δυνατό πλησιέστερα στους πολίτες, και ότι διενεργούνται διαρκείς έλεγχοι ώστε να εξακριβώνεται ότι η δράση σε επίπεδο Ένωσης είναι δικαιολογημένη υπό το φως των διαθέσιμων δυνατοτήτων σε εθνικό, περιφερειακό ή τοπικό επίπεδο. Με άλλα λόγια, είναι η αρχή δυνάμει της οποίας η ΕΕ δεν αναλαμβάνει δράση (εκτός από τους τομείς που εμπίπτουν στην αποκλειστική της αρμοδιότητα), παρά μόνο εφόσον η δράση αυτή είναι πιο αποτελεσματική από την αντίστοιχη δράση σε εθνικό, περιφερειακό ή τοπικό επίπεδο. Είναι άρρηκτα συνδεδεμένη με την αρχή της αναλογικότητας, η οποία απαιτεί να μην υπερβαίνει οποιαδήποτε δράση της ΕΕ όσα είναι αναγκαία για την επίτευξη των στόχων των Συνθηκών.

Πιο συγκεκριμένα, ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης επιβεβαιώνει, λαμβάνοντας υπόψη τις αρμοδιότητες και τις δράσεις της ΕΕ, καθώς και τις προαναφερόμενες αρχές, τα δικαιώματα που προκύπτουν ιδίως από τις κοινές συνταγματικές παραδόσεις και τις κοινές διεθνείς υποχρεώσεις των χωρών της ΕΕ, τη σύμβαση για την προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, τους κοινωνικούς χάρτες που έχουν ψηφιστεί από την ΕΕ και από το Συμβούλιο της Ευρώπης και τη

νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Ο Χάρτης, παρέχοντας διαφάνεια και σαφήνεια στα θεμελιώδη δικαιώματα και ελευθερίες, δημιουργεί νομική ασφάλεια στην ΕΕ.

Στο δεύτερο κεφάλαιο του Χάρτη, το οποίο είναι αφιερωμένο στις Ελευθερίες του Ανθρώπου και πιο συγκεκριμένα, στα άρθρα 7 και 8 αναφέρονται τα ακόλουθα:

Άρθρο 7 (Σεβασμός της ιδιωτικής και οικογενειακής ζωής):

«*Κάθε πρόσωπο έχει το δικαίωμα στο σεβασμό της ιδιωτικής και της οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του*».

Άρθρο 8 (Προστασία δεδομένων προσωπικού χαρακτήρα):

«*1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.*

2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση την συγκατάθεση του ενδιαφερομένου ή για θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει την διόρθωσή τους.

3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής».

2.2 Οδηγία 95/46/ΕΚ (Για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα)

Η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [62], όπως είναι ο πλήρης τίτλος της, συντάχθηκε λαμβάνοντας υπόψη, μεταξύ άλλων, ότι:

Τα συστήματα επεξεργασίας δεδομένων υπηρετούν τον άνθρωπο. Επομένως, πρέπει, ανεξαρτήτως ιθαγένειας ή κατοικίας των φυσικών προσώπων, να σέβονται τις θεμελιώδεις ελευθερίες και τα δικαιώματά τους, και ιδίως την ιδιωτική ζωή και να συμβάλλουν στην οικονομική και κοινωνική πρόοδο, στην ανάπτυξη των εμπορικών συναλλαγών καθώς και στην ευημερία του ατόμου.

Στην Κοινότητα γίνεται όλο και συχνότερη προσφυγή στην επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στους διάφορους τομείς των οικονομικών και κοινωνικών δραστηριοτήτων και η πρόοδος της πληροφορικής διευκολύνει σημαντικά την επεξεργασία και την ανταλλαγή αυτών των δεδομένων.

Οι διαφορές που υπάρχουν στα Κράτη-Μέλη ως προς το επίπεδο προστασίας των δικαιωμάτων και ελευθεριών του ατόμου, και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι δυνατόν να εμποδίζουν τη διαβίβαση των δεδομένων αυτών από το έδαφος ενός στο έδαφος άλλου κράτους μέλους. Οι διαφορές αυτές ενδέχεται συνεπώς να φέρουν εμπόδια στην άσκηση πολλών οικονομικών δραστηριοτήτων σε κοινοτικό επίπεδο, να νοθεύσουν τον ανταγωνισμό και να δυσχεράνουν το έργο των διοικητικών αρχών στο πεδίο εφαρμογής του Κοινοτικού Δικαίου. Αυτές οι διαφορές προστασίας οφείλονται στις αποκλίσεις των εθνικών νομοθετικών, κανονιστικών και διοικητικών διατάξεων.

Για την εξάλειψη των εμποδίων στην κυκλοφορία των Δεδομένων Προσωπικού Χαρακτήρα, πρέπει να υπάρχει ίσος βαθμός προστασίας των δικαιωμάτων και ελευθεριών του ατόμου έναντι της επεξεργασίας των δεδομένων αυτών σε όλα τα Κράτη-Μέλη. Η υλοποίηση αυτού του στόχου που είναι ζωτικός για την εσωτερική αγορά, δεν μπορεί να επιτευχθεί μόνον μέσω των ενεργειών των κρατών μελών, λαμβανομένων ιδίως υπόψη της έκτασης των υφιστάμενων αποκλίσεων μεταξύ των οικείων εθνικών νομοθεσιών καθώς και της ανάγκης συντονισμού των νομοθεσιών των κρατών - μελών, προκειμένου η διασυνοριακή ροή των Δεδομένων Προσωπικού Χαρακτήρα να ρυθμίζεται με συνέπεια και σύμφωνα με τον στόχο της εσωτερικής αγοράς. Ως εκ τούτου, είναι απαραίτητη η παρέμβαση της Κοινότητας ώστε να υπάρξει προσέγγιση των νομοθεσιών.

Έχοντας σαν βάση το παραπάνω σκεπτικό εκδόθηκε η εν λόγω οδηγία, τα κυριότερα σημεία της οποίας είναι τα ακόλουθα:

- Παρουσιάζονται οι αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων.

- Ορίζονται οι βασικές αρχές της νόμιμης επεξεργασίας δεδομένων.
- Αναφέρονται οι ειδικές κατηγορίες επεξεργασίας.
- Γίνεται υποχρεωτική η ενημέρωση του ενδιαφερόμενου προσώπου.
- Δίνεται το δικαίωμα της πρόσβασης του προσώπου στο οποίο αναφέρονται τα δεδομένα.
- Προσδιορίζονται εξαιρέσεις και περιορισμοί .
- Αναλύεται το δικαίωμα της αντίταξης του προσώπου στο οποίο αναφέρονται τα δεδομένα.
- Οριοθετούνται οι έννοιες του Απορρήτου και της Ασφάλειας της επεξεργασίας.
- Δημιουργείται η υποχρέωση κοινοποίησης προς την αρχή ελέγχου.
- Γίνεται αναφορά στα ένδικα μέσα, την έννοια της ευθύνης και τις κυρώσεις.
- Προβλέπονται οι όροι διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες.
- Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας.
- Δίνονται κατευθυντήριες γραμμές γα την σύσταση αρχής ελέγχου και ομάδας για την προστασία των προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ουσιαστικά, η Οδηγία έθεσε βασικές προϋποθέσεις για τη νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα, λαμβάνοντας υπόψη τους κινδύνους που υπάρχουν με την εμφάνιση νέων τεχνολογιών. Η Οδηγία αποτέλεσε το βασικό πυλώνα για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση για πάνω από 20 έτη – αφού κάθε Κράτος-Μέλος την ενσωμάτωσε στην εθνική του νομοθεσία – μέχρι το Μάιο του 2018.

2.3 Νόμος 2472/1997 (Ενσωμάτωση της Οδηγίας 95/46/ΕΚ στο Ελληνικό Δίκαιο)

Με τον νόμο 2472/1997 (ΦΕΚ 50/Α΄/10.04.1997): «Προστασία του ατόμου από την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα» [56], ενσωματώνεται στο ελληνικό δίκαιο η οδηγία 95/46/ΕΚ. Ολόκληρη η σχετική Νομοθεσία βρίσκεται αναρτημένη στην επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου [49], καθώς και στην αντίστοιχη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [47].

Δεν έχει επομένως κανένα νόημα να επαναλάβουμε το σκεπτικό και τις κύριες διατάξεις του νόμου αυτού. Αυτό όμως που οφείλουμε να αναφέρουμε είναι ότι με το συγκεκριμένο νομοθέτημα ιδρύεται στην Ελλάδα η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [47]. Με λίγα λόγια, στον νόμο αυτό ορίζεται η σύσταση, η αποστολή, καθώς και η νομική φύση της εν λόγω αρχής. Επιπλέον, αναφέρονται οι επαγγελματικές ιδιότητες των ατόμων που θα

συγκροτούν την Αρχή (δικαστικοί, καθηγητές ΑΕΙ, κτλ), καθώς επίσης και τα ασυμβίβαστα, οι υποχρεώσεις και τα δικαιώματα των μελών της Αρχής, οι αρμοδιότητες και ο τρόπος λειτουργίας της Αρχής, κοκ.

Αντίστοιχα, και προκειμένου να προσαρμοστεί και η Δημοκρατία της Κύπρου στην εν λόγω νομοθεσία, θέσπισε τον Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμο του 2001. Ο νόμος αυτός εφαρμόζεται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, συμπεριλαμβανομένης της Αστυνομίας και προβλέπει τον διορισμό Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για περίοδο 4 χρόνων, η οποία μπορεί να ανανεωθεί για ακόμα μια περαιτέρω θητεία[48].

Τα καθήκοντα του Επιτρόπου, βάσει του Νόμου, περιλαμβάνουν:

- Την έκδοση οδηγιών, κανόνων, συστάσεων και κωδίκων δεοντολογίας για την προστασία του ατόμου, τη λειτουργία επαγγελματικών σωματείων και τη σωστή διαχείριση των δεδομένων από τους υπεύθυνους επεξεργασίας.
- Τη χορήγηση αδειών που προβλέπονται από το νόμο.
- Τη διεξαγωγή ελέγχων έχοντας για το σκοπό αυτό, δικαίωμα πρόσβασης σε κάθε πληροφορία.
- Την εξέταση παραπόνων σχετικά με την εφαρμογή του Νόμου.
- Την επιβολή κυρώσεων για παραβάσεις του Νόμου.
- Την τήρηση των Μητρώων που προβλέπει ο Νόμος.
- Τη συνεργασία με αντίστοιχες Αρχές άλλων Κρατών-Μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης, σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

2.4 Οδηγία 2002/58/ΕΚ (Προστασία των Δεδομένων Προσωπικού Χαρακτήρα και την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών)

Όπως αναφέραμε και στην αρχή του κεφαλαίου η νομοθεσία, με το πέρασμα του χρόνου, εξελισσόταν συνεχώς προσπαθώντας να ακολουθήσει την τεχνολογική πρόοδο. Έτσι, το 2002 εκδόθηκε η οδηγία 2002/58/ΕΚ [60] «Για την επεξεργασία των δεδομένων προσωπικού

χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών».

Το σκεπτικό για την σύνταξη της οδηγίας αυτής, ήταν να προσαρμοσθεί η Ευρωπαϊκή νομοθεσία στις εξελίξεις των αγορών και των τεχνολογιών των υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να παρέχει το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες.

Από τη μία, η εισαγωγή νέων προηγμένων ψηφιακών τεχνολογιών στα δημόσια δίκτυα επικοινωνίας, δημιουργεί ειδικές απαιτήσεις όσον αφορά την προστασία των Δεδομένων Προσωπικού Χαρακτήρα και της ιδιωτικής ζωής του χρήστη. Η ανάπτυξη της κοινωνίας των πληροφοριών χαρακτηρίζεται από την καθιέρωση νέων υπηρεσιών ηλεκτρονικών επικοινωνιών. Η πρόσβαση σε ψηφιακά κινητά δίκτυα είναι πλέον διαθέσιμη και οικονομικά προσιτή στο ευρύ κοινό. Τα εν λόγω ψηφιακά δίκτυα διαθέτουν σημαντική χωρητικότητα και δυνατότητες επεξεργασίας των προσωπικών δεδομένων. Η επιτυχής διασυνοριακή ανάπτυξη των υπηρεσιών αυτών εξαρτάται, εν μέρει, από την πεποίθηση των χρηστών ότι δεν διακυβεύεται η ιδιωτική τους ζωή.

Από την άλλη, το διαδίκτυο ανατρέπει τις παραδοσιακές δομές της αγοράς παρέχοντας ενιαία, παγκόσμια υποδομή για την παροχή ευρέος φάσματος υπηρεσιών ηλεκτρονικών επικοινωνιών. Οι διαθέσιμες -στο κοινό - υπηρεσίες επικοινωνιών στο διαδίκτυο δημιουργούν νέες δυνατότητες για τους χρήστες, αλλά και νέους κινδύνους για τα προσωπικά τους δεδομένα και την ιδιωτική τους ζωή.

Από όλα τα παραπάνω αντιλαμβανόμαστε πως η νομοθεσία πασχίζει να συμβαδίσει ή έστω να ακολουθήσει εκ του σύνεγγυς, την συνεχώς εξελισσόμενη τεχνολογία. Ενδεικτικές αυτής της προσπάθειας είναι οι τροποποιήσεις που επιδέχθηκε η οδηγία 2002/58/ΕΚ [60] τα επόμενα χρόνια. Γι' αυτό και δεν θα αναλύσουμε στο σημείο αυτό τις κυριότερες διατάξεις της, αλλά θα τις εξετάσουμε στην τελική τους μορφή, στις επόμενες οδηγίες.

Ουσιαστικά, η εν λόγω Οδηγία είναι ειδικότερη της 95/46/ΕΚ για την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, οπότε και – σε αυτές τις περιπτώσεις – εφαρμόζεται αυτή και όχι η 95/46/ΕΚ (αν ένα ζήτημα δεν καλύπτεται από την 2002/58/ΕΚ, τότε προσφεύγουμε στην 95/46/ΕΚ). Η Οδηγία 95/46/ΕΚ τροποποιήθηκε

ακολούθως με την Οδηγία 2009/136/ΕΚ. Κάθε Κράτος-Μέλος έχει ενσωματώσει στην εθνική του νομοθεσία την Οδηγία αυτή.

2.5 Νόμος 3471/2006 (Προστασία Δεδομένων Προσωπικού Χαρακτήρα και της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών)

Ο χαρακτηριστικός τίτλος του νόμου 3471/2006 (ΦΕΚ 133/Α΄/28.06.2006) είναι: «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97» [57]. Όμως, στο πρώτο κεφάλαιο του νόμου διαβάζουμε: « Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002)». Ουσιαστικά, αποτελεί ενσωμάτωση της Οδηγίας 2002/58/ΕΚ στην ελληνική έννομη τάξη.

Αυτή η διττή αναφορά σε προηγούμενη νομοθεσία, μία εθνική και μία ευρωπαϊκή, αποδεικνύει αυτό που έχουμε αναφέρει και προηγουμένως, ότι δηλαδή η ελληνική νομοθεσία έπεται της ευρωπαϊκής και είναι υποχρεωμένη να ενσωματώνει τις ευρωπαϊκές οδηγίες και να προσαρμόζεται σε αυτές.

Στην παρούσα νομοθετική ρύθμιση ορίζονται νομικά οι ακόλουθες έννοιες για τον τομέα των ηλεκτρονικών επικοινωνιών: Απόρρητο, κανόνες επεξεργασίας, δεδομένα κίνησης και θέσης, αναλυτική χρέωση, ένδειξη ταυτότητας και περιορισμός αναγνώρισης, αυτόματη προώθηση κλήσεων, κατάλογοι συνδρομητών, μη ζητηθείσα επικοινωνία, ασφάλεια επεξεργασίας, αστική ευθύνη, ποινικές κυρώσεις. Επιπλέον, προσδιορίζονται οι αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

2.6 Οδηγία 2009/136/ΕΚ (Τροποποίηση της Οδηγίας 2002/58/ΕΚ)

Αν μας ζητούσαν να τεκμηριώσουμε την ανάγκη συνεχούς ανανέωσης και προσαρμογής της νομοθεσίας της ΕΕ, δεν θα μπορούσαμε να βρούμε καλύτερο παράδειγμα από την οδηγία 2009/136/ΕΚ [61]. Ο περιγραφικός της τίτλος το αποδεικνύει: «Για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών».

Αναφορά στην προϋπάρχουσα νομοθεσία της ΕΕ γίνεται και στο σκεπτικό σύνταξης της εν λόγω οδηγίας . Εκεί αναφέρεται ότι η μεταρρύθμιση του πλαισίου κανονιστικών ρυθμίσεων της ΕΕ για δίκτυα και υπηρεσίες ηλεκτρονικών υπηρεσιών, συμπεριλαμβανομένης της ενίσχυσης των διατάξεων για τους τελικούς χρήστες με αναπηρίες, αποτελεί σημαντικό βήμα προς την κατεύθυνση της επίτευξης του Ενιαίου Ευρωπαϊκού Χώρου Πληροφοριών και συγχρόνως, της κοινωνίας της πληροφορίας χωρίς αποκλεισμούς.

Πιο συγκεκριμένα, ορίζεται το θεσμικό πλαίσιο για φωνητικές υπηρεσίες και κοινόχρηστη φωνητική τηλεφωνία, λαμβάνονται μέτρα για τελικούς χρήστες με αναπηρία, προσδιορίζονται οι ρυθμιστικοί έλεγχοι των επιχειρήσεων με σημαντική ισχύ σε συγκεκριμένες λιανικές αγορές, λαμβάνεται πρόνοια για το περιεχόμενο των συμβάσεων των συνδρομητών, οριοθετείται η Διαφάνεια στην δημοσίευση πληροφοριών, αναφέρονται οι παράμετροι μέτρησης της ποιότητας των παρεχόμενων υπηρεσιών, εξασφαλίζεται η διαθεσιμότητα των υπηρεσιών και η ισοτιμία στην πρόσβαση, επιβάλλεται η διευκόλυνση αλλαγής παρόχου, κτλ.

2.7 Νόμος 4070/2012 (Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και Άλλες Διατάξεις)

Στο νόμο 4070/2012(ΦΕΚ 82/Α΄/10.04.2012) [58] με τίτλο: «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις», καθορίζεται το πλαίσιο παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών. Επιπλέον, αναφέρεται σαφώς ότι η Εθνική Ρυθμιστική Αρχή (National Regulator Authority), σε θέματα παροχής δικτύων και

υπηρεσιών ηλεκτρονικών επικοινωνιών, είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.). Μεγάλο τμήμα του παρόντος νόμου έχει αφιερωθεί στον ορισμό του τρόπου λειτουργίας της Ε.Ε.Τ.Τ (άρθρο 6 και εξής), καθώς και στην παρουσίαση του φάσματος των αρμοδιοτήτων της.

Επίσης, σε ακόμη μία προσπάθεια συμμόρφωσης με το ευρωπαϊκό δίκαιο, στο έκτο τμήμα (μέρος ΣΤ΄ - άρθρο 168 και εξής) του εν λόγω νόμου, αναφέρονται οι: «Διατάξεις του Υπουργείου Δικαιοσύνης για την ενσωμάτωση στην εθνική έννομη τάξη της οδηγίας 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009, κατά το μέρος που αφορά την τροποποίηση της οδηγίας 2002/58/ΕΚ, σχετικά με την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα και της προστασίας της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών».

Άρα, αυτός ο νόμος τροποποίησε, μεταξύ άλλων, κατάλληλα το ν. 3471/2006, υπό την ίδια έννοια που η Οδηγία 2009/136/ΕΚ τροποποίησε την Οδηγία 2002/58/ΕΚ. Στο νόμο αυτό ρυθμίζεται, μεταξύ άλλων, το ζήτημα της εγκατάστασης και περαιτέρω επεξεργασίας των cookies στους τερματικούς εξοπλισμούς των χρηστών.

2.8 Κανονισμός (ΕΕ) 2013/611 της Επιτροπής (Εφαρμοστέα Μέτρα για την Κοινοποίηση Παραβιάσεων Προσωπικών Δεδομένων Βάσει της Οδηγίας 2002/58/ΕΚ)

Ο κανονισμός (ΕΕ) 2013/611 [53] της Επιτροπής της 24ης Ιουνίου 2013 «σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες», εφαρμόζεται στην κοινοποίηση των παραβιάσεων των Δεδομένων Προσωπικού Χαρακτήρα από τους παρόχους των, διαθέσιμων στο κοινό, υπηρεσιών ηλεκτρονικών επικοινωνιών.

Πιο συγκεκριμένα, ορίζει την διαδικασία κοινοποίησης τόσο στην αρμόδια Εθνική Αρχή, όσο και στον συνδρομητή, αλλά και σε άλλο πάροχο (αν υπάρχει τέτοια σύμβαση), σε περίπτωση παραβίασης των Δεδομένων Προσωπικού Χαρακτήρα. Επίσης γίνεται αναφορά στα

τεχνολογικά μέσα προστασίας που δύναται να εφαρμόσει ο πάροχος, όπως είναι η κρυπτογράφηση των δεδομένων, ώστε, σε περίπτωση παραβίασης, τα δεδομένα αυτά να είναι ακατανόητα σε οποιοδήποτε πρόσωπο δεν διαθέτει το δικαίωμα πρόσβασης σε αυτά.

2.9 Κανονισμός (ΕΕ) 2016/679 (Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών)

Ο κανονισμός (ΕΕ) 2016/679 [54] 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 – General Data Protection Regulation (GDPR))», είναι ο πλέον πρόσφατος που πραγματεύεται το ζήτημα της προστασίας των Δεδομένων Προσωπικού Χαρακτήρα στην Ευρωπαϊκή Ένωση.

Πρόκειται για το αποτέλεσμα επίπονων διαβουλεύσεων μεταξύ των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης, των κρατών μελών της, αλλά και διεθνών οργανισμών και επιχειρήσεων, η λειτουργία των οποίων άπτεται της δικαιοδοσίας του εν λόγω κανονισμού. Η εφαρμογή του θεωρείται ύψιστης σημασίας, επειδή φέρει πολλές καινοτομίες και γι' αυτό θα του αφιερώσουμε το επόμενο κεφάλαιο της παρούσας μεταπτυχιακής διατριβής.

2.10 Οδηγία (ΕΕ) 2016/680 (Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές…)

Η οδηγία (ΕΕ) 2016/680 [59] 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 και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου», έρχεται να ρυθμίσει τις σχέσεις των κρατών – μελών της ΕΕ με τους πολίτες τους, υπό το πρίσμα της προστασίας των δικαιωμάτων των πολιτών.

Πιο συγκεκριμένα, η παρούσα οδηγία θεσπίζει τους κανόνες που αφορούν στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

Αναλυτικότερα, η εν λόγω οδηγία προσδιορίζει, μεταξύ άλλων: Τις προθεσμίες αποθήκευσης και διαγραφής των δεδομένων, τις κατηγορίες των υποκειμένων και των δεδομένων, την νομιμότητα της επεξεργασίας, τις ειδικές κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα, τα δικαιώματα του υποκειμένου των δεδομένων, την συνεργασία με την αρμόδια εποπτική Αρχή.

Επίκειται ενσωμάτωση της Οδηγίας αυτής σε κάθε εθνική νομοθεσία στα Κράτη-Μέλη (στην Ελλάδα, το σχετικό σχέδιο νόμου τέθηκε σε δημόσια διαβούλευση το Μάρτιο του 2018: ο νόμος δεν είχε ακόμα κατατεθεί στο Κοινοβούλιο στο διάστημα που γράφονται οι γραμμές αυτές).

Κεφάλαιο 3
Κανονισμός (ΕΕ) 2016/679 – Ευκαιρίες και Προκλήσεις

Στο συγκεκριμένο κεφάλαιο θα παρουσιάσουμε κάποια από τα κυριότερα σημεία του κανονισμού (ΕΕ) 2016/679 [54] 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», ο οποίος είναι γνωστός με την πιο σύντομη ονομασία: Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) – General Data Protection Regulation (GDPR). Επιπλέον, στο Παράρτημα Α θα παρουσιάσουμε τον πίνακα περιεχομένων του ΓΚΠΔ, ώστε ο κάθε ενδιαφερόμενος να είναι σε θέση να εντοπίσει άμεσα το άρθρο που τον αφορά.

3.1 Εισαγωγή στον Γενικό Κανονισμό για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Είναι αλήθεια ότι τα τελευταία δύο έτη, δηλαδή από την ψήφιση του εν λόγω κανονισμού το 2016 έως και την στιγμή συγγραφής της παρούσας μεταπτυχιακής διατριβής (μιας και η προθεσμία συμμόρφωσης των κρατών – μελών λήγει στις 25 Μαΐου) , έχει χυθεί πολύ μελάνι τόσο από τον νομικό κόσμο, όσο και από τον τομέα της τεχνολογίας.

Σκοπός του ΓΚΠΔ [19] είναι η προστασία όλων των πολιτών της ΕΕ από παραβιάσεις του απορρήτου και των δεδομένων, σε έναν κόσμο που τροφοδοτείται με δεδομένα σε ολοένα και μεγαλύτερο βαθμό και ο οποίος παρουσιάζει τεράστιες διαφορές από την εποχή κατά την οποία θεσπίστηκε η οδηγία του 1995 [62]. Παρότι οι βασικές αρχές τήρησης απορρήτου των δεδομένων, εξακολουθούν να ισχύουν με βάση τα όσα ορίζονται στην προηγούμενη οδηγία, έχει προταθεί πληθώρα αλλαγών ως προς τις σχετικές ρυθμιστικές πολιτικές.

Αναμφίβολα, η μεγαλύτερη αλλαγή στο ρυθμιστικό τοπίο, σχετικά με την τήρηση απορρήτου των δεδομένων αναφέρεται στη διεύρυνση του πεδίου αρμοδιότητας του ΓΚΠΔ, καθώς εφαρμόζεται σε όλες τις επιχειρήσεις που επεξεργάζονται Δεδομένα Προσωπικού Χαρακτήρα που προέρχονται από τα Υποκείμενα των Δεδομένων αυτών και τα οποία διαμένουν εντός της Ευρωπαϊκής Ένωσης, ασχέτως του τόπου εγκατάστασης της επιχείρησης. Προηγουμένως, η δυνατότητα εφαρμογής της οδηγίας κατά τόπους ήταν αμφισβητούμενη και αναφερόταν στην επεξεργασία δεδομένων εντός του πλαισίου αναφοράς ενός φορέα: αν για παράδειγμα μία εταιρεία είχε εγκατάσταση στη χώρα Α της Ευρωπαϊκής Ένωσης αλλά επεξεργαζόταν δεδομένα όλων των Ευρωπαίων πολιτών (π.χ. παρέχοντας υπηρεσίες κοινωνικής δικτύωσης), τότε μόνο η Αρχή Προστασίας Δεδομένων της χώρας Α είχε αρμοδιότητα επί της εν λόγω επεξεργασίας. Περαιτέρω, αν δεν υπήρχε εγκατάσταση σε καμία χώρα της ΕΕ, τότε καμία ευρωπαϊκή νομοθεσία δεν είχε αρμοδιότητα. Το ζήτημα αυτό έχει ανακύψει σε έναν αριθμό υποθέσεων που εμπίπτουν στην αρμοδιότητα των ανώτατων δικαστηρίων. Ο ΓΚΠΔ καθιστά πολύ σαφή τα όρια της δυνατότητας εφαρμογής του.

Έτσι, ο ΓΚΠΔ θα εφαρμόζεται κατά την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα, από τα πρόσωπα που είναι αρμόδια για τον έλεγχο και επεξεργασία δεδομένων εντός της ΕΕ, ασχέτως εάν η επεξεργασία λαμβάνει χώρα εντός της ΕΕ ή όχι. Ο ΓΚΠΔ θα ισχύει επίσης κατά την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα ατόμων, στα οποία αναφέρονται τα δεδομένα αυτά, εντός της ΕΕ, εκ μέρους του προσώπου που είναι αρμόδιο για τον έλεγχο ή την επεξεργασία και το οποίο δεν είναι εγκατεστημένο εντός της ΕΕ. Οι δραστηριότητες αυτές σχετίζονται με: την παροχή προϊόντων ή υπηρεσιών προς πολίτες της ΕΕ (ασχέτως εάν απαιτείται πληρωμή) και την παρακολούθηση συμπεριφοράς που λαμβάνει χώρα εντός της ΕΕ. Επιχειρήσεις εκτός της ΕΕ, οι οποίες προβαίνουν σε επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα πολιτών της ΕΕ, θα πρέπει επίσης να διορίζουν αντιπρόσωπο εντός της ΕΕ.

Ειδική αναφορά πρέπει να γίνει και στον ορισμό του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer – DPO), ο οποίος διορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία, βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων. Υπεύθυνο Προστασίας Δεδομένων υποχρεούνται να διορίσουν τόσο δημόσιες αρχές και φορείς, όσο και επιχειρήσεις οι οποίες επεξεργάζονται Δεδομένα Προσωπικού Χαρακτήρα. Το πρόσωπο αυτό μπορεί να είναι μέλος του προσωπικού του Υπευθύνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία (οι οποίοι έχουν και την υποχρέωση να δημοσιεύουν τα στοιχεία επικοινωνίας του και τα ανακοινώνουν στην εποπτική αρχή), ή να ασκεί τα καθήκοντά του

βάσει σύμβασης παροχής υπηρεσιών. Τα καθήκοντά του, σε γενικές γραμμές, είναι να ενημερώνει και συμβουλεύει τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία, αλλά και τους υπαλλήλους που επεξεργάζονται δεδομένα για τις υποχρεώσεις τους που απορρέουν από τον ΓΚΠΔ, να παρακολουθεί την συμμόρφωση με τον ΓΚΠΔ, να συνεργάζεται με την εποπτική αρχή και να ενεργεί ως σημείο επικοινωνίας μεταξύ αυτής και του εργοδότη του.

Μία ακόμη βασική καινοτομία είναι ότι σε περίπτωση παραβίασης Δεδομένων Προσωπικού Χαρακτήρα, ο Υπεύθυνος Επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης των Δεδομένων Προσωπικού Χαρακτήρα στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση Δεδομένων Προσωπικού Χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην αρμόδια εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Επιπλέον εισάγεται η έννοια της «προστασίας των προσωπικών δεδομένων εκ του Σχεδιασμού» (data protection by design). Η συγκεκριμένη έννοια υπάρχει εδώ και χρόνια, αλλά, στο πλαίσιο του ΓΚΠΔ αποτελεί πλέον νομική υποχρέωση. Σύμφωνα με αυτήν, απαιτείται η ενσωμάτωση της προστασίας δεδομένων από την έναρξη ακόμη του σχεδιασμού των συστημάτων, παρά με τη μορφή εκ των υστέρων προσθήκης. Πιο συγκεκριμένα, ήδη κατά τη σχεδίαση μιας επεξεργασίας (π.χ. μιας εφαρμογής ή ενός συστήματος), θα πρέπει να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε με αποτελεσματικό τρόπο, να πληρούνται οι απαιτήσεις του εν λόγω Κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων και όχι μετά τη σχεδίασή του να εξετάζεται αν πληρούνται οι προϋποθέσεις νομιμότητας έτσι ώστε, εάν όχι, να γίνεται τότε προσπάθεια διορθωτικών μέτρων. Επίσης, στο ίδιο άρθρο 25 του ΓΚΠΔ τίθεται η απαίτηση για την τήρηση και επεξεργασία μόνο των Δεδομένων Προσωπικού Χαρακτήρα εκείνων, που είναι απολύτως απαραίτητα για την εκπλήρωση του σκοπού της επεξεργασίας (ελαχιστοποίηση των δεδομένων –αρχή της αναλογικότητας), καθώς επίσης και τον περιορισμό της πρόσβασης σε Δεδομένα Προσωπικού Χαρακτήρα σε εκείνα, τα οποία θεωρούνται ως απαραίτητα για την ολοκλήρωση της εκτέλεσης της επεξεργασίας. Αυτό ονομάζεται «προστασία των δεδομένων εξ ορισμού» (data protection by default): για παράδειγμα, σε υπηρεσίες κοινωνικής δικτύωσης, αυτό συνεπάγεται ότι οι προκαθορισμένες ρυθμίσεις θα πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα. Όπως θα δούμε και στο επόμενο κεφάλαιο, οι έννοιες της προστασίας των δεδομένων κατά τη σχεδίαση και εξ ορισμού είναι πολύ σημαντικές για τις m-health εφαρμογές.

Με την έναρξη ισχύος του ΓΚΠΔ, οι οργανισμοί που παραβαίνουν τον εν λόγω κανονισμό μπορεί να τιμωρηθούν με πρόστιμο έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών τους ή 20 εκατομμύρια ευρώ (όποιο από τα δύο είναι μεγαλύτερο). Αυτό είναι το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις, όπως είναι π.χ. η μη λήψη επαρκούς συγκατάθεσης του πελάτη για επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα ή η παράβαση των βασικών διατάξεων που αναφέρονται στις έννοιες τήρησης Ιδιωτικού Απορρήτου εκ του Σχεδιασμού. Υπάρχει μία κλιμακωτή προσέγγιση ως προς τα πρόστιμα. Π.χ. μία επιχείρηση μπορεί να τιμωρηθεί με πρόστιμο 2% για τη μη τήρηση των αρχείων της με τάξη (άρθρο 28 του ΚΚΠΔ), μη ενημέρωση της εποπτεύουσας αρχής και του προσώπου στο οποίο αναφέρονται τα δεδομένα, σχετικά με κάποια παράβαση ή μη πραγματοποίηση αξιολόγησης επιπτώσεων. Θα πρέπει να τονιστεί ιδιαίτερα, ότι οι εν λόγω κανονισμοί ισχύουν τόσο για τα πρόσωπα που είναι αρμόδια για τον έλεγχο, όσο και για αυτά που είναι αρμόδια για την επεξεργασία — πράγμα που σημαίνει ότι τυχόν ασαφή σημεία δεν θα εξαιρούνται κατά την εφαρμογή του ΓΚΠΔ.

Ο ΓΚΠΔ επίσης προάγει την έννοια της διαφάνειας της επεξεργασίας προσωπικών δεδομένων, υπό την έννοια ότι όσοι επεξεργάζονται προσωπικά δεδομένα πρέπει να παρέχουν ακόμα αναλυτικότερες πληροφορίες επ' αυτής στα πρόσωπα των οποίων τα δεδομένα υφίστανται επεξεργασία: στο ίδιο πλαίσιο, ο ΓΚΠΔ αποσαφηνίζει πλήρως την έννοια της σαφούς, ρητής και ειδικής συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων (τονίζοντας ρητά, μεταξύ άλλων, ότι πρέπει να προκύψει με σαφή θετική ενέργεια του χρήστη, και ότι απλά η σιωπηρή αποδοχή όρων δεν συνιστά συγκατάθεση, ούτε επίσης είναι έγκυρη η μία ενιαία συγκατάθεση για πολλούς διαφορετικούς σκοπούς). Οι έννοιες αυτές έχουν σημασία για τις εφαρμογές m-health που μελετώνται στην παρούσα διατριβή.

3.2 Επεξήγηση Όρων Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Για να γίνουν κατανοητές οι διατάξεις του ΓΚΠΔ από όλους, κρίνεται σκόπιμο να εξηγήσουμε κάποιους βασικούς ορισμούς, οι οποίοι χρησιμοποιούνται ευρύτατα σε αυτόν.

3.2.1 Απλά Δεδομένα Προσωπικού Χαρακτήρα – Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα

Ως «Δεδομένο Προσωπικού Χαρακτήρα» νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. 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 online 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.

Αντίστοιχα, τα γνωστά στο ευρύ κοινό ως «Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα» [20] αναφέρονται στον ΓΚΠΔ ως «Ειδικές Κατηγορίες Δεδομένων» που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η 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. Τα δεδομένα αυτά προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά Δεδομένα Προσωπικού Χαρακτήρα.

Οι ειδικές κατηγορίες δεδομένων (ευαίσθητα δεδομένα) που εμφανίζουν ιδιαίτερο ενδιαφέρον για την παρούσα μεταπτυχιακή διατριβή είναι τα «Δεδομένα που αφορούν την υγεία». Πρόκειται για Δεδομένα Προσωπικού Χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

Συμπληρωματικά αναφέρονται τα «Γενετικά Δεδομένα», τα οποία είναι τα Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

Τέλος, δεν μπορούμε να παραλείψουμε και τα «Βιομετρικά Δεδομένα». Πρόκειται για Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα

οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

Από τα παραπάνω συμπεραίνουμε ότι τα Γενετικά και Βιομετρικά Δεδομένα είναι Ευαίσθητα Δεδομένα, την προστασία των οποίων προβλέπει ο ΓΚΠΔ, σε αντίθεση με την (παλαιότερη) οδηγία 95/46/ΕΚ που δεν τα περιελάμβανε σε αυτά.

3.2.2 Επεξεργασία Δεδομένων

Με τον όρο «Επεξεργασία Δεδομένων» εννοούμε κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε Δεδομένα Προσωπικού Χαρακτήρα ή σε σύνολα Δεδομένων Προσωπικού Χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

3.2.3 Υπεύθυνος Επεξεργασίας

Ο «Υπεύθυνος Επεξεργασίας» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο Υπεύθυνος Επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους - μέλους.

3.2.4 Εκτελών την Επεξεργασία

Ο «Εκτελών την Επεξεργασία» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται Δεδομένα Προσωπικού Χαρακτήρα για λογαριασμό του Υπευθύνου της Επεξεργασίας.

3.2.5 Υποκείμενο των Δεδομένων

Το Υποκείμενο των Δεδομένων είναι στην ουσία το φυσικό πρόσωπο (ταυτοποιημένο ή ταυτοποιήσιμο), στο οποίο αναφέρονται τα δεδομένα. Για την επεξεργασία των δεδομένων είναι απαραίτητη η συγκατάθεσή του. Με τον όρο συγκατάθεση εννοούμε κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το Υποκείμενο των Δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα Δεδομένα Προσωπικού Χαρακτήρα που το αφορούν.

3.3 Θεμελιώδεις Αρχές που διέπουν την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Οι θεμελιώδεις αρχές που διέπουν την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα, απαριθμούνται στο άρθρο 5 του ΓΚΠΔ. Σύμφωνα με αυτές, τα Δεδομένα Προσωπικού Χαρακτήρα:

- Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο, σε σχέση με το υποκείμενο των δεδομένων (Αρχή της Νομιμότητας, Αντικειμενικότητας και Διαφάνειας).
- Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς (Αρχή της Αναλογικότητας ή Αρχή Περιορισμού του Σκοπού).
- Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (Αρχή Ελαχιστοποίησης των Δεδομένων).
- Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση Δεδομένων Προσωπικού Χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας (Αρχή της Ακρίβειας).
- Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των Υποκειμένων των Δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα. Επίσης, μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα Δεδομένα Προσωπικού Χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής

έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 του ΓΚΠΔ και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων (Αρχή Περιορισμός της Περιόδου Αποθήκευσης).

- Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των Δεδομένων Προσωπικού Χαρακτήρα, 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 (Αρχή της Ακεραιότητας και της Εμπιστευτικότητας).
- Ο Υπεύθυνος Επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις Αρχές που διέπουν την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα, σύμφωνα με την παράγραφο 1 του άρθρου 5 του ΓΚΠΔ (Αρχή της Λογοδοσίας).

3.4 Δικαιώματα του Υποκειμένου

Τα Δικαιώματα του Υποκειμένου περιγράφονται στο τρίτο κεφάλαιο του ΓΚΠΔ. Κάποια από αυτά είχαν θεσμοθετηθεί και σε προηγούμενη νομοθεσία και εδώ απλά τροποποιούνται για να ανταποκρίνονται στις σημερινές απαιτήσεις, ενώ κάποια άλλα θα τα συναντήσουμε για πρώτη φορά. Γενικότερα, ο ΓΚΠΔ σαφώς ενισχύει τα δικαιώματα των υποκειμένων των δεδομένων.

3.4.1 Το Δικαίωμα της Ενημέρωσης

Ο Υπεύθυνος Επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία ή/και ανακοίνωση σχετικά με την επεξεργασία, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το Υποκείμενο των Δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του Υποκειμένου των Δεδομένων είναι αποδεδειγμένη με άλλα μέσα. Επιπλέον, προβλέπονται οι διαδικασίες Ενημέρωσης του Υποκειμένου για τις περιπτώσεις όπου τα Δεδομένα Προσωπικού Χαρακτήρα έχουν συλλεγεί από το Υποκείμενο των Δεδομένων ή από άλλη πηγή.

3.4.2 Το Δικαίωμα της Πρόσβασης

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να λαμβάνει από τον Υπεύθυνο Επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα Δεδομένα Προσωπικού Χαρακτήρα που το αφορούν υφίστανται επεξεργασία. Εάν συμβαίνει αυτό, τότε λαμβάνει επίσης και το Δικαίωμα της Πρόσβασης στα Δεδομένα Προσωπικού Χαρακτήρα που έχουν συλλεχθεί και το αφορούν. Ο Υπεύθυνος Επεξεργασίας παρέχει αντίγραφο των Δεδομένων Προσωπικού Χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το Υποκείμενο των Δεδομένων, ο Υπεύθυνος Επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Εάν το Υποκείμενο των Δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το Υποκείμενο των Δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

3.4.3 Το Δικαίωμα της Διόρθωσης

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να απαιτήσει από τον Υπεύθυνο Επεξεργασίας, χωρίς αδικαιολόγητη καθυστέρηση, την διόρθωση ανακριβών Δεδομένων Προσωπικού Χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το Υποκείμενο των Δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών Δεδομένων Προσωπικού Χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

3.4.4 Το Δικαίωμα της Αντίρρησης - Εναντίωσης

Το Υποκείμενο των Δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα που το αφορούν, περιλαμβανομένης της κατάρτισης προφίλ, βάσει των εν λόγω διατάξεων. Ο Υπεύθυνος Επεξεργασίας δεν υποβάλλει πλέον τα Δεδομένα Προσωπικού Χαρακτήρα σε επεξεργασία, εκτός εάν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του Υποκειμένου των Δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Εάν Δεδομένα Προσωπικού Χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το Υποκείμενο των Δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα που το αφορούν, για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

3.4.5 Το δικαίωμα Περιορισμού της Επεξεργασίας

Το Υποκείμενο των Δεδομένων δικαιούται να εξασφαλίζει από τον Υπεύθυνο Επεξεργασίας τον περιορισμό της επεξεργασίας, όταν για παράδειγμα: α) η ακρίβεια των Δεδομένων Προσωπικού Χαρακτήρα αμφισβητείται από το Υποκείμενο των Δεδομένων, για χρονικό διάστημα που επιτρέπει στον Υπεύθυνο Επεξεργασίας να επαληθεύσει την ακρίβεια των Δεδομένων Προσωπικού Χαρακτήρα, β) η επεξεργασία είναι παράνομη και το Υποκείμενο των Δεδομένων αντιτάσσεται στη διαγραφή των Δεδομένων Προσωπικού Χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους, γ) ο Υπεύθυνος Επεξεργασίας δεν χρειάζεται πλέον τα Δεδομένα Προσωπικού Χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το Υποκείμενο των Δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων, κτλ.

3.4.6 Το Δικαίωμα στην Λήθη

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να ζητήσει από τον Υπεύθυνο Επεξεργασίας τη διαγραφή Δεδομένων Προσωπικού Χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο Υπεύθυνος Επεξεργασίας υποχρεούται να διαγράψει Δεδομένα Προσωπικού Χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν για παράδειγμα: Δεν είναι πλέον απαραίτητα, υποβλήθηκαν σε επεξεργασία παράνομα, το Υποκείμενο των Δεδομένων ανακαλεί την συγκατάθεσή του, κοκ.

Όταν ο Υπεύθυνος Επεξεργασίας έχει δημοσιοποιήσει τα Δεδομένα Προσωπικού Χαρακτήρα και υποχρεούται να τα διαγράψει, τότε, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους Εκτελούντες την Επεξεργασία που διαχειρίζονται τα Δεδομένα Προσωπικού Χαρακτήρα, ότι το Υποκείμενο των Δεδομένων ζήτησε τη διαγραφή τυχόν συνδέσμων με τα

δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω Δεδομένων Προσωπικού Χαρακτήρα.

3.4.7 Το δικαίωμα στην Φορητότητα των Δεδομένων

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να λαμβάνει τα Δεδομένα Προσωπικού Χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε Υπεύθυνο Επεξεργασίας, σε δομημένη, κοινώς χρησιμοποιούμενη και αναγνώσιμη από μηχανήματα μορφή, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον Υπεύθυνο Επεξεργασίας, χωρίς αντίρρηση από τον Υπεύθυνο Επεξεργασίας στον οποίο παρασχέθηκαν αρχικά τα Δεδομένα Προσωπικού Χαρακτήρα.

3.4.8 Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων, Περιλαμβανομένης της Κατάρτισης Προφίλ

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

3.4.9 Ρητή και Σαφή Συγκατάθεση του Υποκειμένου για Επεξεργασία των Δεδομένων του

Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο Υπεύθυνος Επεξεργασίας είναι σε θέση να αποδείξει ότι το Υποκείμενο των Δεδομένων συγκατατέθηκε για την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα που το αφορούν.

Εάν η συγκατάθεση του Υποκειμένου των Δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής, το οποίο συνιστά παράβαση του παρόντος κανονισμού, δεν είναι δεσμευτικό.

Το Υποκείμενο των Δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το Υποκείμενο των Δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

Για την εκτίμηση του βαθμού ελευθερίας απόδοσης της συγκατάθεσης, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης (όπως η παροχή μιας υπηρεσίας), τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

3.4.10 Υποχρέωση Γνωστοποίησης Όσον Αφορά την Διόρθωση ή την Διαγραφή Δεδομένων Προσωπικού Χαρακτήρα ή τον Περιορισμό της Επεξεργασίας ή των Περιστατικών Παραβίασης Δεδομένων

Ο Υπεύθυνος Επεξεργασίας οφείλει να ανακοινώνει κάθε διόρθωση ή διαγραφή Δεδομένων Προσωπικού Χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων, σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα Δεδομένα Προσωπικού Χαρακτήρα, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια. Ο Υπεύθυνος Επεξεργασίας ενημερώνει το Υποκείμενο των Δεδομένων σχετικά με τους εν λόγω αποδέκτες, εφόσον αυτό ζητηθεί από το ίδιο το Υποκείμενο των Δεδομένων.

Επιπλέον, όταν διαπιστωθεί περιστατικό παραβίασης Δεδομένων Προσωπικού Χαρακτήρα , το οποίο ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Υπεύθυνος Επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των Δεδομένων Προσωπικού Χαρακτήρα στο Υποκείμενο των Δεδομένων.

3.5 Κρυπτογράφηση των Δεδομένων

Προκειμένου να διαφυλαχθεί η ασφάλεια της επεξεργασίας των δεδομένων και λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Υπεύθυνος Επεξεργασίας και ο Εκτελών την Επεξεργασία εφαρμόζουν κατάλληλα

τεχνικά και οργανωτικά μέτρα (προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων), περιλαμβανομένων, μεταξύ άλλων, την ψευδωνυμοποίηση και την κρυπτογράφηση των Δεδομένων Προσωπικού Χαρακτήρα.

3.6 Γονική Συναίνεση

Όταν η προσφορά υπηρεσιών , σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθύνεται απευθείας σε παιδί, η επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα παιδιού είναι σύννομη εάν το παιδί είναι τουλάχιστον 16 χρονών. Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού. Τα κράτη - μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία για τους εν λόγω σκοπούς, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία δεν είναι κάτω από τα 13 έτη. Ο Υπεύθυνος Επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία.

Χαρακτηριστικό παράδειγμα συμμόρφωσης [43] αποτελεί η εφαρμογή WhatsApp, η οποία, σύμφωνα με στοιχεία του Φεβρουαρίου του 2018 χρησιμοποιείται από περισσότερους από 1,5 δισ. ανθρώπους, καθιστώντας την την μεγαλύτερη στον τομέα των επικοινωνιών στον πλανήτη. Η εφαρμογή WhatsApp λοιπόν, απαγορεύει την πρόσβαση σε όλους όσους είναι κάτω των 16 ετών στην Ευρωπαϊκή Ένωση και κατ' επέκταση, στην Ελλάδα και την Κύπρο.

Η εφαρμογή του μέτρου θα ξεκινήσει από τις 25 Μαΐου 2018. Συγκεκριμένα, οι χρήστες στην Ευρώπη κατά την είσοδο τους στην εφαρμογή whatsApp θα καλούνται να επιβεβαιώσουν την ηλικία τους, κατά την διαδικασία αποδοχής των νέων Όρων Χρήσης και την ανανεωμένη Πολιτική Ασφάλειας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα. Εκτός Ευρώπης η κατώτερη ηλικία χρήσης του whatsApp παραμένει τα 13 χρόνια.

Το whatsApp, το οποίο είναι εταιρεία του ομίλου της Facebook, διαθέτει διαφορετική πολιτική Δεδομένων Προσωπικού Χαρακτήρα σε σχέση με το κοινωνικό δίκτυο. Η προσέγγιση του Facebook για συμμόρφωση με τους νέους κανόνες θα είναι να ζητήσει από τους έφηβους ηλικίας 13 έως 15 ετών να αποκτήσουν γονική άδεια για την ανταλλαγή προσωπικών πληροφοριών

στην πλατφόρμα. Αν δεν λάβουν την σχετική άδεια, θα δουν μια πιο γενική έκδοση του Facebook που δεν έχει προσαρμοστεί με βάση τα δεδομένα τους.

Από τα παραπάνω αντιλαμβανόμαστε πόσο σημαντική θεωρούν την συμμόρφωση με τον ΓΚΠΔ εταιρείες-κολοσσοί , όπως η Facebook. Ο προβληματισμός όμως που (υπήρχε και) παραμένει είναι το πως μία διαδικτυακή υπηρεσία ελέγχει το «γνήσιον» της ηλικίας.

Κεφάλαιο 4
Ηλεκτρονική Υγεία – Η Περίπτωση των «Έξυπνων Εφαρμογών»

Στο κεφάλαιο αυτό εξετάζουμε τα ζητήματα που εγείρονται από τις απαιτήσεις προστασίας προσωπικών δεδομένων στον τομέα της υγείας και, ειδικότερα, της ηλεκτρονικής υγείας. Αναλυτικότερα, θα παρουσιαστεί ο Κώδικας Ιατρικής Δεοντολογίας, δίνοντας έμφαση στα σημεία εκείνα που ορίζουν την διαχείριση των Δεδομένων Προσωπικού Χαρακτήρα των ασθενών. Ακόμη, αναλύονται τα ζητήματα που προκύπτουν από την εφαρμογή του ΓΚΠΔ, όσον αφορά την προστασία των Δεδομένων Προσωπικού Χαρακτήρα στον τομέα της Ηλεκτρονικής Υγείας. Πιο συγκεκριμένα, εδώ μελετάται η περίπτωση των «έξυπνων» εφαρμογών στην Ηλεκτρονική Υγεία, δίνοντας έμφαση στις εφαρμογές mobile health (m-health applications) και το πώς αυτές διαχειρίζονται τα Δεδομένα Προσωπικού Χαρακτήρα των χρηστών.

4.1 Κώδικας Ιατρικής Δεοντολογίας(Νόμος 3418/2005)

Ο χώρος της υγείας διαχειρίζεται και Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα, τα οποία ο ΓΚΠΔ (άρθρο 4) κατατάσσει στις «Ειδικές Κατηγορίες Δεδομένων». Πρόκειται για: Δεδομένα υγείας, γενετικά δεδομένα, βιομετρικά δεδομένα, αλλά και δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό. Τα δεδομένα αυτά προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά Δεδομένα Προσωπικού Χαρακτήρα.

Η ελληνική πολιτεία, με βάση το άρθρο 27 της οδηγίας 95/46/ΕΚ [62], εξέδωσε τον νόμο 3418/2005 (ΦΕΚ 287/Α΄/28.11.2005): «Κώδικας Ιατρικής Δεοντολογίας» ο οποίος, στο άρθρο 14, ορίζει για την τήρηση του ιατρικού αρχείου τα ακόλουθα:

Ο ιατρός υποχρεούται να τηρεί ιατρικό αρχείο, σε ηλεκτρονική ή μη μορφή, το οποίο περιέχει δεδομένα που συνδέονται αρρήκτως ή αιτιωδώς με την ασθένεια ή την υγεία των ασθενών του. Για την τήρηση του αρχείου αυτού και την επεξεργασία των δεδομένων του εφαρμόζονται οι διατάξεις του νόμου 2472/1997 (ΦΕΚ 50/Α΄/10.04.1997) [56].

Τα ιατρικά αρχεία πρέπει να περιέχουν το ονοματεπώνυμο, το πατρώνυμο, το φύλο, την ηλικία, το επάγγελμα, τη διεύθυνση του ασθενή, τις ημερομηνίες της επίσκεψης, καθώς και κάθε άλλο ουσιώδες στοιχείο που συνδέεται με την παροχή φροντίδας στον ασθενή, όπως, ενδεικτικά και ανάλογα με την ειδικότητα, τα ενοχλήματα της υγείας του και το λόγο της επίσκεψης, την πρωτογενή και δευτερογενή διάγνωση ή την αγωγή που ακολουθήθηκε.

Οι κλινικές και τα νοσοκομεία τηρούν στα ιατρικά τους αρχεία και τα αποτελέσματα όλων των κλινικών και παρακλινικών εξετάσεων.

Η υποχρέωση διατήρησης των ιατρικών αρχείων ισχύει: α) στα ιδιωτικά ιατρεία και τις λοιπές μονάδες πρωτοβάθμιας φροντίδας υγείας του ιδιωτικού τομέα, για μία δεκαετία από την τελευταία επίσκεψη του ασθενή και β) σε κάθε άλλη περίπτωση, για μία εικοσαετία από την τελευταία επίσκεψη του ασθενή.

Ο ιατρός λαμβάνει όλα τα αναγκαία μέτρα, έτσι ώστε στην περίπτωση επιστημονικών δημοσιεύσεων να μην γνωστοποιείται με οποιονδήποτε τρόπο η ταυτότητα του ασθενή στον οποίο αφορούν τα δεδομένα. Εάν, λόγω της φύσης της δημοσίευσης, είναι αναγκαία η αποκάλυψη της ταυτότητας του ασθενή ή στοιχείων που υποδεικνύουν ή μπορούν να οδηγήσουν στην εξακρίβωση της ταυτότητάς του, απαιτείται η ειδική έγγραφη συναίνεσή του.

Ο ιατρός τηρεί τα επαγγελματικά του βιβλία με τέτοιο τρόπο, ώστε να εξασφαλίζεται το ιατρικό απόρρητο και η προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

Στα ιατρικά αρχεία δεν πρέπει να αναγράφονται κρίσεις ή σχολιασμοί για τους ασθενείς, παρά μόνον εάν αφορούν στην ασθένειά τους.

Ο ασθενής έχει δικαίωμα πρόσβασης στα ιατρικά αρχεία, καθώς και λήψης αντιγράφων του φακέλου του. Το δικαίωμα αυτό, μετά το θάνατό του, ασκούν οι κληρονόμοι του, εφόσον είναι συγγενείς μέχρι τετάρτου βαθμού.

Δεν επιτρέπεται σε τρίτο η πρόσβαση στα ιατρικά αρχεία ασθενή. Κατ' εξαίρεση επιτρέπεται η πρόσβαση: α) στις δικαστικές και εισαγγελικές αρχές κατά την άσκηση των καθηκόντων τους αυτεπάγγελτα ή μετά από αίτηση τρίτου που επικαλείται έννομο συμφέρον και σύμφωνα με τις νόμιμες διαδικασίες, β) σε άλλα όργανα της Ελληνικής Πολιτείας, που με βάση τις καταστατικές τους διατάξεις έχουν τέτοιο δικαίωμα και αρμοδιότητα.

Ο ασθενής έχει το δικαίωμα πρόσβασης, σύμφωνα με τις οικείες διατάξεις, στα εθνικά ή διεθνή αρχεία στα οποία έχουν εισέλθει τα Δεδομένα Προσωπικού Χαρακτήρα που τον αφορούν.

Παρατηρούμε ότι ο ισχύων Κώδικας Ιατρικής Δεοντολογίας βασίζεται σε παλαιότερη οδηγία. Αυτό συμβαίνει μιας και η δεσμευτική ημερομηνία ισχύς του ΓΚΠΔ είναι η 25/5/2018. Αναμένεται λοιπόν η προσαρμογή του παρόντος Κώδικα Δεοντολογίας στις ρήσεις του ΓΚΠΔ. Η ειδοποιός διαφορά του ΓΚΠΔ, σε σχέση με την οδηγία 95/46/ΕΚ, είναι ότι σε αυτόν έχουν προστεθεί στα δεδομένα υγείας τα γενετικά και βιομετρικά δεδομένα, σε μια ακόμη προσπάθεια προσαρμογής της νομοθεσίας στις τεχνολογικές εξελίξεις.

4.2 Ηλεκτρονική Υγεία στην Ελλάδα

Η Ηλεκτρονική Υγεία (e-health) είναι ένας αναδυόμενος τομέας στη διασταύρωση της ιατρικής πληροφορικής, της δημόσιας υγείας και των επιχειρήσεων, που αναφέρεται στις υπηρεσίες υγείας και στις πληροφορίες που παρέχονται ή ενισχύονται μέσω του Διαδικτύου και των συναφών τεχνολογιών. Με μια ευρύτερη έννοια, ο όρος χαρακτηρίζει όχι μόνο μια τεχνική εξέλιξη, αλλά και έναν τρόπο σκέψης, μία στάση ζωής και μία δέσμευση για δικτυωμένη, παγκόσμια σκέψη, για τη βελτίωση της υγειονομικής περίθαλψης σε τοπικό, περιφερειακό και παγκόσμιο επίπεδο με τη χρήση τεχνολογίας πληροφοριών και επικοινωνιών [32].

Το 2000, η ελληνική κυβέρνηση, σύμφωνα με τις συστάσεις της Ευρωπαϊκής Ένωσης για την Κοινωνία της Πληροφορίας, εξασφάλισε ένα επιχειρησιακό πρόγραμμα για την εφαρμογή της στρατηγικής της Κοινωνίας της Πληροφορίας στην Ελλάδα, με συνεκτικό και ολοκληρωμένο τρόπο. Κατά την περίοδο 2000-2006, στο πλαίσιο του 3ου Κοινοτικού Πλαισίου Στήριξης (ΚΠΣ), η Ελλάδα ξεκίνησε την ανάπτυξη Ολοκληρωμένων Πληροφοριακών Συστημάτων Υγείας (ΟΠΣΥ) για την πλειοψηφία των - τότε - δεκαεπτά Περιφερειακών Διευθύνσεων Υγείας. 83 από τα 132 νοσοκομεία της Ελλάδας καλύπτονταν από το πρόγραμμα και απέκτησαν Ολοκληρωμένα Πληροφοριακά Συστήματα μέσω της Περιφερειακής Διεύθυνσης Υγείας στην οποία ανήκαν. Η

μεγάλη αξία του Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας είναι ότι επιτρέπουν την κατανεμημένη συλλογή ιατρικών και κλινικών δεδομένων ως μέρος των διαδικασιών εργασίας και αποτελεσματική πρόσβαση στο Ηλεκτρονικό Φάκελο Υγείας (ΗΦΥ) [35].

Ο Ηλεκτρονικός φάκελος Υγείας (ΗΦΥ) θεωρείται η «καρδιά» των κλινικών πληροφοριακών συστημάτων, η οποία μετουσιώνει τους παραδοσιακούς ιατρικούς φακέλους, δίνοντάς τους μια νέα μορφή: ηλεκτρονική, ασφαλή, απόρρητη, προσβάσιμη μόνο από τους εξουσιοδοτημένους γιατρούς ή ασθενείς και ενοποιημένη με άλλα είδη ηλεκτρονικών πηγών, υπηρεσιών και πληροφοριών. Πλέον ψηφιακά αρχεία που συνδέονται με ένα διαδικτυακό σύστημα πληροφοριών παγκόσμιας εμβέλειας μας δίνουν τη δυνατότητα να έχουμε άμεση μεταφορά των δεδομένων σε οποιεσδήποτε εγκαταστάσεις υγείας ανά τον κόσμο βρίσκεται ο ασθενής δίνοντας άμεσα μια πλήρης εικόνα της υγείας του. Απώτερος σκοπός είναι η δημιουργία ενός πλήρους ιατρικού αρχείου του οποίου η ηλεκτρονική μορφή θα βοηθήσει στην αυτοματοποίηση και οργάνωση των υπηρεσιών στα κέντρα υγείας. Το αποτέλεσμα αυτής της διαδικασίας επιδιώκεται να είναι οι ασφαλέστερες αποφάσεις που βασίζονται σε αντικειμενικά στοιχεία για τον ασθενή και η ποιότητα στη διοίκηση για το ίδιο το σύστημα υγείας.

Επιπλέον, ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) έχει καθιερωθεί ως ο αριθμός αναγνώρισης όλων των πολιτών στην Ελλάδα, στον τομέα της απασχόλησης και της κοινωνικής ασφάλισης. Έχει χρησιμοποιηθεί στο Σύστημα της Ηλεκτρονικής Συνταγογράφησης (ePrescription) και θα χρησιμοποιηθεί και στον Ηλεκτρονικό Φάκελο Υγείας (ΗΦΥ). Η χρήση του Αριθμού Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) στα υπάρχοντα Ολοκληρωμένα Πληροφοριακά Συστήματα Υγείας (ΟΠΣΥ) διευκολύνει την σύνδεση των πληροφοριών των ασθενών.

Η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[47] ασχολήθηκε με το ζήτημα των υποχρεώσεων που σχετίζονται με την ασφάλεια, σε σχέση με τα ηλεκτρονικά ιατρικά αρχεία των υπαλλήλων και καθόρισε τις ελάχιστες προδιαγραφές της ηλεκτρονικής εφαρμογής που χρησιμοποιείται από τον γιατρό εργασίας, κατά την επεξεργασία του ιατρικού φακέλου του ασθενούς. Τα κύρια σημεία αφορούν: Την κρυπτογράφηση των Ευαίσθητων Δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων, την αυστηρή πρόσβαση μόνο στον γιατρό εργασίας και στους βοηθούς του, που υπόκεινται στις ίδιες υποχρεώσεις του επαγγελματικού (εδώ ιατρικού) απορρήτου ή τους σχετικούς Κώδικες Δεοντολογίας, την ασφαλή αναγνώριση και τους μηχανισμούς ελέγχου της ταυτότητας των χρηστών, την ασφάλεια στην ανάπτυξη συστημάτων και στο δίκτυο που φιλοξενεί την εφαρμογή, την

εφαρμογή των αρχείων καταγραφής (log files), την ύπαρξη πολιτικής για τη δημιουργία αντιγράφων ασφάλειας, την ασφαλή καταστροφή των Δεδομένων Προσωπικού Χαρακτήρα, τα φυσικά μέτρα για την ασφάλεια των συστημάτων πληροφορικής και τέλος, την ενημέρωση των εργαζομένων για την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα που τους αφορούν και τον τρόπο με τον οποίο να ασκήσουν το Δικαίωμα της Πρόσβασης. Η εν λόγω απόφαση δημοσιεύθηκε στην ετήσια έκθεση της Αρχής του 2012 (αρ. πρωτ: ΓΝ/ΕΞ/6301/03-10-2012, κεφ: 3.3.3 «Υγεία – Νέες τεχνολογίες/Ηλεκτρονικά μέσα», σελ. 71-72), κατόπιν σχετικού ερωτήματος του Σώματος Επιθεώρησης Εργασίας (ΣΕΠΕ).

Τέλος, όταν γίνεται λόγος για τις μορφές της Ηλεκτρονικής Υγείας στην Ελλάδα, οφείλουμε να αναφέρουμε και την Τηλεϊατρική. Ο Παγκόσμιος Οργανισμός Υγείας, αναφέρει ότι: *Η Τηλεϊατρική είναι η παροχή υπηρεσιών υγειονομικής φροντίδας σε απόσταση, από επαγγελματίες υγείας που χρησιμοποιούν ΤΠΕ για τη μεταφορά και τη λήψη σημαντικών πληροφοριών διάγνωσης, θεραπείας και πρόληψης ασθενών τραυματισμών , για την έρευνα , τη συνεχιζόμενη εκπαίδευση με τη προώθηση της υγείας των ατόμων και των κοινωνιών*. Όσο αυξάνονται οι δυνατότητες της τεχνολογίας, τόσο αυξάνονται και οι δυνατότητες εφαρμογής της Τηλεϊατρικής. Η Τηλεϊατρική είναι πολλαπλά χρήσιμη γιατί: παρέχει ισότητα στη πρόσβαση των υπηρεσιών υγείας, εγγυάται την ποιότητα, ανταποκρίνεται στις δημογραφικές μεταβολές, βοηθάει στη βελτίωση του θεραπευτικού αποτελέσματος, προάγει την έρευνα και την τεχνολογία, βοηθάει στη περιστολή των δαπανών και προσφέρει επιχειρηματικές δυνατότητες. Είναι ακόμη ιδιαίτερα χρήσιμη σε περιπτώσεις επαναληπτικών επισκέψεων, όπου ο ιατρός θέλει απλά να ελέγξει την πορεία της επιλεγμένης θεραπείας.

Ενδεικτικό παράδειγμα των μεγάλων δυνατοτήτων που προσφέρει η Τηλεϊατρική αποτελεί το δίκτυο HYGEIAnet στην Κρήτη. Πρόκειται για το πρώτο ολοκληρωμένο περιφερειακό δίκτυο τηλεματικών εφαρμογών στην υγεία, το οποίο διασυνδέει όλους τους φορείς του ΕΣΥ στην περιφέρεια της Κρήτης. Η μεγάλη του συμβολή έγκειται στο γεγονός ότι δίνει τη δυνατότητα να αντιμετωπιστεί έγκαιρα ένα επείγον περιστατικό στα τοπικά ιατρεία από γιατρούς γενικής ιατρικής, σύμφωνα με τις οδηγίες που τους δίνουν εξ αποστάσεως ειδικευμένοι γιατροί. Σε περίπτωση που η κατάσταση του ασθενούς θεωρηθεί κρίσιμη, η θεραπευτική αγωγή μπορεί να ξεκινήσει άμεσα υπό την καθοδήγηση του ειδικού ενώ μπορεί να δρομολογηθεί και η ασφαλής διακομιδή του από το ΕΚΑΒ σε κατάλληλη εντατική μονάδα. Πληροφορίες μπορούν να δίνονται και κατά τη μεταφορά του ασθενούς με το ασθενοφόρο, καθώς όλες οι κινητές μονάδες του ΕΚΑΒ συνδέονται με το συντονιστικό κέντρο. Με αυτόν τον τρόπο, το νοσοκομείο ενημερώνεται άμεσα για την κατάσταση του ασθενούς ενώ ειδικευμένοι γιατροί δίνουν τις κατάλληλες οδηγίες

στο πλήρωμα της κινητής μονάδας. Καθίσταται, λοιπόν, αντιληπτό πως η χρήση υπηρεσιών τηλεϊατρικής εξοικονομεί πολύτιμο χρόνο στην αντιμετώπιση των περιστατικών και παρέχει συνεχόμενη φροντίδα στους ασθενείς[35].

4.3 «Έξυπνες» Εφαρμογές Υγείας και Ασφάλεια Δεδομένων

Ο ορισμός που αποδίδεται στις «Έξυπνες» εφαρμογές υγείας (ευρέως γνωστή ως Mobile Health και εν συντομία m-Health) από τον Παγκόσμιο Οργανισμό Υγείας (Π.Ο.Υ.) είναι: «Η άσκηση της ατομικής και δημόσιας υγείας από φορητές συσκευές όπως κινητά τηλέφωνα, συσκευές παρακολούθησης του ασθενή και άλλες ασύρματες συσκευές» (WHO, 2009). Αργότερα, στον όρο m-Health προστέθηκαν και οι κατάλληλες εφαρμογές κινητής τηλεφωνίας που έχουν σχεδιαστεί προκειμένου να προωθήσουν έναν υγιεινό τρόπο ζωής στον πληθυσμό, μία ατομική καθοδήγηση στην προσωπική παρακολούθηση της κατάστασης του ασθενούς από τον ίδιο, υπενθυμίσεις φαρμακοληψίας και την άμεση επικοινωνία του ασθενή με τον θεράποντα ιατρό του [07].

Οι m-Health εφαρμογές μπορούμε να πούμε ότι είναι το μέλλον της περίθαλψης, καθώς επιτρέπουν στον ασθενή να μένει ενεργός και ταυτόχρονα υπεύθυνος, αλλά και να διευκολύνει τη δουλειά του ιατρού, κάνοντας την περισσότερο αποτελεσματική. Φυσικά, αφορμή για να αποκτήσει ένα τόσο μεγάλο ενδιαφέρον το m-Health είναι η ραγδαία ανάπτυξη των δυνατοτήτων των «έξυπνων» κινητών τηλεφώνων (smartphones), με τη παράλληλη ευρεία αποδοχή και χρήση τους από το καταναλωτικό κοινό. Έτσι δίνεται η δυνατότητα της χρήσης των παραπάνω εφαρμογών σε ένα πολύ μεγάλο κομμάτι του πληθυσμού.

Αυτή η δυνατότητα της μαζικής διείσδυσης του m-Health στη κοινωνία σε συνδυασμό με το καινοτόμο του χαρακτήρα του είναι που θα προκαλέσει σημαντικές αλλαγές σε όλο το φάσμα της κοινωνίας τα επόμενα χρόνια. Από οικονομικής άποψης, η ανάπτυξη του m-Health θα μειώσει την αυξανόμενη δημοσιονομική πίεση των συστημάτων περίθαλψης των κρατών λόγω προκλήσεων της σύγχρονης εποχής όπως η γήρανση του πληθυσμού κ.α.. Από κοινωνικής άποψης, οι υπηρεσίες m-Health αναμένεται να συμβάλλουν στην καθιέρωση υγειονομικής περίθαλψης που θέτει περισσότερο τον ασθενή στο επίκεντρο, και στην υποστήριξη της στροφής προς την πρόληψη και στην ταυτόχρονη βελτίωση της αποτελεσματικότητας του συστήματος υγείας.

Δεν πρέπει να ξεχνάμε όμως, ότι το m-Health έχει να αντιμετωπίσει σοβαρές προκλήσεις όσον αφορά ζητήματα νομικού περιεχόμενου πχ. Την τήρηση και Διαχείριση των Δεδομένων Προσωπικού Χαρακτήρα του ασθενή. Τα ζητήματα αυτά θα προσπαθήσουμε να περιγράψουμε ακολούθως.

4.3.1 Ερευνητικό Υπόβαθρο

Τα τελευταία χρόνια έχει παρατηρηθεί μία «έκρηξη» στην κινητή υπολογιστική (mobile computing) και την προοδευτική της υιοθέτηση στις καθημερινές δραστηριότητες των ανθρώπων. Μία νέα αγορά λογισμικού, αυτή των κινητών εφαρμογών (mobile apps) αναπτύσσεται συνεχώς, με τον κάθε δημιουργό λειτουργικού συστήματος κινητής (mobile OS) να επιδιώκει να έχει την δική του ανεξάρτητη αγορά. Αναμφίβολα, μία από τις πιο δημοφιλείς κατηγορίες λογισμικού, σε αυτά τα online καταστήματα, είναι αυτή της υγείας και του ευ ζην. Παράλληλα, οι προγραμματιστές και οι διαφημιστές προωθούν την αύξηση της αγοράς των m-Health εφαρμογών[12].

Υπάρχει μία διαφαινόμενη στροφή προς το μοντέλο της «συνδεδεμένης υγείας» (“connected health”), [46] όπου ο στόχος είναι η επίτευξη ευέλικτων, αποτελεσματικών και προσιτών υπηρεσιών παροχής υγείας, ακολουθώντας το παράδειγμα της – βασισμένης στο περιεχόμενο – ευφυούς υγείας (context aware smart health: s-health) [03],[04]. Σε αυτό το τεχνολογικό περιβάλλον, όπου πολλές συσκευές μοιράζονται κοινές πλατφόρμες λειτουργικών συστημάτων, οι mobile εφαρμογές συχνά θεωρούνται μέρος του Internet of Things (IoT) οικοσυστήματος [06], [36] και επομένως, ενδέχεται να «πάσχουν» από παρόμοιες αδυναμίες. Παρ’ όλα αυτά, ένας αυξανόμενος αριθμός επαγγελματιών της υγείας στρέφονται προς την χρήση των mobile εφαρμογών για καλύτερη επικοινωνία και διαχείριση των Δεδομένων Υγείας των ασθενών τους. Ευκολία, καλύτερη λήψη κλινικών αποφάσεων, βελτιωμένη ακρίβεια, αυξανόμενη αποτελεσματικότητα και ενισχυμένη παραγωγικότητα [07], είναι μόνο μερικά από τα οφέλη που οι mobile εφαρμογές παρέχουν στους επαγγελματίες υγείας. Ως αποτέλεσμα, υπάρχει αυξανόμενο ενδιαφέρον για mobile προσβάσιμα προσωπικά αρχεία υγείας, τα οποία επιτρέπουν στους παρόχους υπηρεσιών υγείας καλύτερο «μοίρασμα» πληροφοριών με τους ασθενείς[30].

Αυτή η αξιοσημείωτη ανάπτυξη της m-Health αγοράς, εντούτοις, συμβαδίζει με μία αυξανόμενη ανησυχία για την ετοιμότητα των κινητών συσκευών (π.χ. smartphones, tablets) και των

εφαρμογών που εγκαθίσταται σε αυτές, όσον αφορά την Ασφάλεια και την Ιδιωτικότητα. Μία αναφορά της Ευρωπαϊκής Επιτροπής για την προστασία των δεδομένων των πολιτών στα 28 Κράτη-Μέλη της ΕΕ [38] επιβεβαιώνει ότι πάνω από τους μισούς από όσους ερωτήθηκαν, στις 16 χώρες όπου πραγματοποιήθηκε η σχετική έρευνα, δήλωσαν ότι ήταν ανήσυχοι για την καταγραφή των καθημερινών δραστηριοτήτων τους μέσω της χρήσης του κινητού τους τηλεφώνου ή mobile εφαρμογών. Ανταποκρινόμενη – μεταξύ άλλων - στις ανησυχίες των πολιτών για την ανεπαρκή και ασαφή προστασία των προσωπικών τους δεδομένων στην εποχή της ολοκληρωτικής επικράτησης των υπολογιστών, η Ευρωπαϊκή Επιτροπή προχώρησε στην σύνταξη του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ) [54]. Ο εν λόγω Κανονισμός επιβάλλει, όπως είδαμε στο Κεφάλαιο 3, νέες νομικές απαιτήσεις στους Υπεύθυνους Επεξεργασίας Δεδομένων οι οποίοι δραστηριοποιούνται εντός της ΕΕ και προβλέπει αυστηρές κυρώσεις για τις περιπτώσεις μη συμμόρφωσης με τις διατάξεις του.

Ωστόσο, οι ανησυχίες για τις m-Health εφαρμογές δεν περιορίζονται μόνο στον χώρο της ΕΕ. Στις Ηνωμένες Πολιτείες της Αμερικής για παράδειγμα, υπάρχει σκεπτικισμός για το κατά πόσο είναι εφαρμόσιμα τα εθνικά πρότυπα (US Standards) του οργανισμού για την Ασφάλιση Υγείας και την Λογοδοσία (Health Insurance Portability and Accountability Act – HIPAA), ο οποίος ορίζει τις πολιτικές, τις διαδικασίες και τις κατευθυντήριες γραμμές για την διατήρηση της Ιδιωτικότητας και της Ασφάλειας για τα ατομικά, ταυτοποιήσιμα δεδομένα υγείας. Είναι άξιον λόγου το γεγονός ότι αρκετοί μελετητές επιχειρηματολογούν ότι οι m-Health εφαρμογές αποτυγχάνουν να συμμορφωθούν με τον κανονισμό προστασίας του HIPAA[10].

Ως επιβεβαίωση των παραπάνω, μπορούμε να αναφέρουμε κάποιες ενδεικτικές μελέτες στο εν λόγω ζήτημα. Μία μελέτη σχετικά με την Ασφάλεια και την Ιδιωτικότητα ανέλυσε 43 εφαρμογές υγείας και ευ ζην, οι οποίες είχαν αναπτυχθεί για λειτουργικά συστήματα iOS και Android [08]. Οι ερευνητές διαπίστωσαν ότι 40% των εφαρμογών κατέδειξαν υψηλό κίνδυνο για την Ιδιωτικότητα του χρήστη, 32% μέτριο προς υψηλό και 28% χαμηλό προς μέτριο. Καμία από τις εφαρμογές αυτές δεν κατέδειξε μηδενικό κίνδυνο. Αντίθετα, εντοπίστηκαν τρεις κύριες τεχνικές αιτίες για τους κινδύνους στην Ιδιωτικότητα στις εφαρμογές m-Health: Μη κρυπτογραφημένη κυκλοφορία δεδομένων, ενσωματωμένες διαφημίσεις και υπηρεσίες τρίτων μερών για ανάλυση/ιχνηλάτηση χρηστών.

Σε ένα άλλο άρθρο [10], οι ερευνητές κατέταξαν 160 εφαρμογές m-Health, οι οποίες είναι διαθέσιμες στο Google Play, με σκοπό να διαμορφώσουν μία λίστα από 7 κατηγορίες επιθέσεων οι οποίες πρέπει να λαμβάνονται υπόψη όταν πραγματοποιείται η αξιολόγηση μίας εφαρμογής

για να διαπιστωθεί το επίπεδο Ασφάλειας και Ιδιωτικότητας αυτής. Οι κατηγορίες αυτές είναι: Το διαδίκτυο, υπηρεσίες τρίτων, Bluetooth, logging, αποθήκευση σε κάρτα SD, εξαγόμενα στοιχεία και «παράπλευρα κανάλια» (side channels). Τυχαία δείγματα εφαρμογών δοκιμάστηκαν και αναλύθηκαν υπό το πρίσμα των 7 προαναφερόμενων κατηγοριών, δίνοντας ιδιαίτερη έμφαση στο διαδίκτυο και στις υπηρεσίες τρίτων. Σύμφωνα με τα αποτελέσματα, 63,6% των εφαρμογών έστελναν μη κρυπτογραφημένα δεδομένα στο διαδίκτυο και το 81,8% χρησιμοποιούσαν υπηρεσίες τρίτων για την αποθήκευση και την φιλοξενία, όπως οι υπηρεσίες cloud του Amazon.

Οι παραπάνω μελέτες αντικατοπτρίζουν τις μείζονες ανησυχίες που προκύπτουν από τον τρόπο που η κάθε m-Health εφαρμογή συλλέγει, διαχειρίζεται, ή/και μοιράζει τις ιδιωτικές πληροφορίες των χρηστών. Για παράδειγμα, θα τίθεται πάντοτε θέμα εμπιστοσύνης όταν μία εφαρμογή θα συλλέγει περισσότερες πληροφορίες από όσες της είναι απαραίτητες για να παρέχει τις υπηρεσίες της, παραβιάζοντας έτσι τις αρχές της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού που αναφέρονται στον ΓΚΠΔ. Επιπλέον, όσον αφορά την ασφάλεια στην συνδεσιμότητα, είναι πολύ συνηθισμένο σήμερα για τους χρήστες να χρησιμοποιούν μη ασφαλή δίκτυα (π.χ. καταστήματος, εστιατορίου, αεροδρομίου, κτλ) για την πρόσβασή τους σε mobile εφαρμογές, και επομένως, δεν είναι δυνατή η απόδοση ευθυνών για διαρροή πληροφοριών σε συγκεκριμένα δίκτυα.

4.3.2 Ζητήματα Ασφάλειας m-Health εφαρμογών

ΟΙ κίνδυνοι που διατρέχουν η Ιδιωτικότητα και η Προστασία των Δεδομένων στις mobile εφαρμογές προέρχονται κυρίως από δύο διαστάσεις: α) Την ίδια τους τη φύση, ως λογισμικό που εκτελείται σε ιδιωτικές κινητές συσκευές χρηστών (φορητές συσκευές – handheld devices) και β) τις ιδιαιτερότητες του περιβάλλοντος της ανάπτυξης και της διανομής των κινητών, αυτό καθεαυτό. Πιο αναλυτικά, οι κατηγορίες των σχετικών κινδύνων, αλλά και παραγόντων κινδύνων είναι:

Ποικιλία δεδομένων και πολλαπλοί αισθητήρες:

Οι κινητές συσκευές μπορούν τυπικά να έχουν πρόσβαση σε διάφορους τύπους προσωπικών/ευαίσθητων δεδομένων (π.χ. υγείας, κλινικά δεδομένα) που παρέχονται από τους χρήστες μέσω διαφόρων mobile εφαρμογών. Επιπλέον, οι τυπικές φορητές συσκευές έχουν ενσωματωμένους πολλούς και διάφορους αισθητήρες (π.χ. μικρόφωνο, κάμερα, επιταχυνσιόμετρο, GPS, Wi-Fi, κτλ), οι οποίοι με τη σειρά τους παράγουν πολλά προσωπικά και

ποικίλα δεδομένα και μεταδεδομένα (metadata), όπως: Τοποθεσία, χρόνο, θερμοκρασία και τα οποία μπορεί να έχουν απροσδόκητες επιπτώσεις στην Ιδιωτικότητα. Για παράδειγμα, έχει αποδειχθεί ότι οι χρήστες μπορούν εύκολα να εντοπιστούν και να επικυρωθούν από τα σήματα κίνησης που έχουν αποκτηθεί από smartphone, όπως σήματα επιταχυνσιόμετρου και γυροσκοπίου (αδρανειακά) που παρέχονται από τα περισσότερα εμπορικά smartphones [27]. Ομοίως, έχει αποδειχθεί ότι οι κινητές συσκευές μπορούν μερικές φορές να παρακολουθούνται από την χωρητικότητα της μπαταρίας τους [26].

Προσωπικές συσκευές - μόνιμα σε λειτουργία:

Οι χρήστες πολύ συχνά βλέπουν ένα smartphone ή ένα tablet σαν επέκταση του εαυτού τους και τείνουν να το θεωρούν ως μία αξιόπιστη, πολύ προσωπική συσκευή, την οποία δεν θα μοιράζονται με κανέναν. Επιπλέον, τέτοιες συσκευές είναι σχεδόν πάντοτε ενεργοποιημένες, μεταφέρονται σχεδόν παντού από τον χρήστη τους και συνδέονται σε ένα δίκτυο. Συνήθως οι χρήστες αποθηκεύουν στις συσκευές αυτές πολλά προσωπικά δεδομένα για μεγάλο χρονικό διάστημα. Αυτό τους κάνει τέλειους στόχους για τους λεγόμενους «μεσίτες» δεδομένων (databrokers), τους διαφημιζόμενους ή τους ανιχνευτές εν γένει και μπορεί να οδηγήσει σε διαδεδομένη και συνεχόμενη παρακολούθηση των χρηστών. Αυτή είναι η έννοια της «ρευστής παρακολούθησης» (liquid surveillance), όπου και οι μικρότερες λεπτομέρειες της καθημερινής μας ζωής παρακολουθούνται και ανιχνεύονται [46]. Επίσης, οι χρήστες είναι όλο και περισσότερο συνηθισμένοι στην δυνατότητα του φωνητικού ελέγχου, υποστηριζόμενη σε μέσα φωνητικής ανάλυσης όπως το Siri, το Google Now, ή το Contana. Ωστόσο, οι χρήστες δεν έχουν επίγνωση του γεγονότος ότι η λειτουργία φωνητικού ελέγχου πραγματοποιείται από μία συσκευή που ακούει πάντα – τουλάχιστον για να αντιδρά στους ορισμένους όρους ελέγχου όπως “Hey Siri”, “Okay Google”, ή “Hey Contana” - και ως εκ τούτου, έχει πρόσβαση σε όλες τις ομιλούμενες επικοινωνίες[27].

Διαφορετικοί τύποι αναγνωριστικών:

Οι κινητές συσκευές περιέχουν πολλούς και διαφορετικούς τύπους αναγνωριστικών (αναγνωριστικό υλικού συσκευής, αποθηκευμένα αρχεία και μεταδεδομένα), ή δακτυλικών αποτυπωμάτων, (διαμόρφωσης [02] ή συμπεριφοράς δακτυλικά αποτυπώματα [24]), τα οποία μπορούν να χρησιμοποιηθούν από mobile εφαρμογές για την ταυτοποίηση και την παρακολούθησή τους[34]. Παραδείγματος χάριν, μία έρευνα έδειξε ότι τέσσερα χωρο-χρονικά σημεία, προερχόμενα πιθανώς από smartphone, είναι αρκετά ώστε να ταυτοποιήσουν π.χ. να αναγνωρίσουν μονοσήμαντα το 95% των ατόμων[45]. Επίσης, μία αλλά έρευνα έδειξε ότι οποιεσδήποτε 4 εφαρμογές, οι οποίες είναι εγκατεστημένες από έναν χρήστη στην συσκευή

του/της, είναι αρκετές ώστε να τον/την ταυτοποιήσουν με μία πιθανότητα 95%[23]. Τα περισσότερα από τα αναγνωριστικά αυτά, όπως τα συμπεριφορικά δακτυλικά αποτυπώματα (behavioural fingerprints), είναι συνήθως μόνιμα και είναι δύσκολο – αν όχι ακατόρθωτο – να γίνει επαναφορά τους (reset).

Κινητά και συνδεσιμότητα στο διαδίκτυο:

Οι κινητές συσκευές μπορούν να εντοπιστούν γεωγραφικά και να παρακολουθούνται φυσικά. Το χαρακτηριστικό αυτό μπορεί να έχει σημαντικές επιπτώσεις στην Ιδιωτικότητα. Στην πραγματικότητα, πολλές, ενδεχομένως, ευαίσθητες προσωπικές πληροφορίες (π.χ. θρησκεία, ασθένεια) θα μπορούσαν να συναχθούν για ένα άτομο από το ίχνος του κινητού του/της [01]. Επιπλέον, δεδομένου ότι είναι κινητές συσκευές, μπορούν να συνδεθούν σε διαφορετικά, ενδεχομένως κακόβουλα, δίκτυα τα οποία εισάγουν νέους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα[44].

Δυνατότητα παρακολούθησης:

Όπως είδαμε προηγουμένως, οι φορητές συσκευές μπορούν να παρακολουθούνται φυσικά μέσω των ασύρματων διεπαφών από τρίτους (third-parties) για την δημιουργία φυσικών προφίλ [24]. Μπορούν επίσης να παρακολουθούνται από τρίτους όταν συνδέονται στο διαδίκτυο. Πολλά τρίτα μέρη πραγματοποιούν την παρακολούθηση εφαρμόζοντας πρακτικές συνδυασμού πληροφορίας από διάφορες πηγές (cross-domain), όπως για παράδειγμα: να συνδυάζουν τα φυσικά και τα online προφίλ των χρηστών[09]. Αυτή η cross-domain παρακολούθηση μπορεί να παρέχει μία πιο πλήρη εικόνα της συμπεριφοράς του χρήστη και εισάγει νέους κινδύνους για την Ασφάλεια και την Ιδιωτικότητα. Αντίστοιχη παρακολούθηση μπορεί να γίνει συνδυάζοντας πληροφορίες από περισσότερες από μία συσκευές (cross-device tracking) [25], [41], όπου τρίτα μέρη προσπαθούν να συνδέσουν μαζί τις συσκευές που ανήκουν σε ένα χρήστη, καθώς επίσης και συνδυάζοντας πληροφορίες από διαφορετικές εφαρμογές (cross-app tracking) [23], όπου μία εφαρμογή προσπαθεί να αναγνωρίσει/παρακολουθήσει τις υπόλοιπες εγκατεστημένες εφαρμογές σε μία συσκευή. Οι πρακτικές αυτές είναι εξίσου επεκτεινόμενες και εισάγουν καινούργιες και πολύ σοβαρές ανησυχίες για την Ιδιωτικότητα. Για παράδειγμα, έχει αποδειχθεί ότι χαρακτηριστικά γνωρίσματα του χρήστη, όπως: θρησκεία, κατάσταση σχέσης, ομιλούντες γλώσσες, χώρες ενδιαφέροντος και το εάν ο χρήστης είναι γονιός μικρού παιδιού ή όχι, μπορεί να προβλεφθεί από ένα υποσύνολο από την λίστα εφαρμογών του κινητού του/της[37].

Περιορισμένη φυσική ασφάλεια:

Οι φορητές συσκευές είναι συχνά μικρές - σε φυσικό μέγεθος – συσκευές, οι οποίες είναι δύσκολο να ασφαλιστούν. Μπορούν εύκολα να κλαπούν ή να χαλάσουν και αυτό μπορεί να έχει αντίκτυπο στην Εμπιστευτικότητα, αλλά και στην Διαθεσιμότητα των δεδομένων. Επίσης, πολλές πηγές κινδύνων (σύντροφοι, σύζυγοι, συγγενείς) μπορούν να έχουν φυσική πρόσβαση σε αυτές, τους αισθητήρες τους ή συσχετισμένες υπηρεσίες.

Περιορισμένες διεπαφές χρήστη:

Οι φορητές συσκευές έχουν συνήθως περιορισμένες διεπαφές χρήστη (User Interfaces – UI). Αυτό, φυσικά, επηρεάζει την Ιδιωτικότητα, την Διαφάνεια και την Ασφάλεια. Παραδείγματος χάριν, μία μελέτη έδειξε ότι οι κωδικοί πρόσβασης που δημιουργούνται σε κινητές συσκευές είναι αδύναμοι[42]. Η Πολιτική Απορρήτου και οι ειδοποιήσεις είναι πολύ πιο δύσκολο να διαβαστούν σε ένα smartphone και απαιτούν πολύ προσοχή. Σαν αποτέλεσμα, οι Πολιτικές Απορρήτου θα πρέπει να οικοδομούνται χρησιμοποιώντας μια προσέγγιση διαστρωμάτωσης, όπου τα πιο σημαντικά σημεία θα παρουσιάζονται συνοπτικά και θα υπάρχουν περισσότερες λεπτομέρειες - εύκολα προσβάσιμες- εάν ο χρήστης θέλει να τις δει. Επιπρόσθετα, ένας καλός σχεδιασμός των γραφικών, ο οποίος θα περιλαμβάνει χρώματα και σύμβολα, μπορεί να βοηθήσει τους χρήστες να κατανοήσουν καλύτερα μία Πολιτική Απορρήτου[40].

Περιορισμοί των προγραμματιστών των εφαρμογών:

Οι mobile εφαρμογές συχνά αναπτύσσονται από ένα μεμονωμένο άτομο ή μία μικρή ομάδα ανθρώπων, οι οποίοι έχουν περιορισμένους πόρους και εμπειρία στην Ασφάλεια και την Ιδιωτικότητα. Επομένως, είναι δύσκολο για τους προγραμματιστές να υιοθετήσουν τις τελευταίες τεχνικές λύσεις για την προστασία της Ιδιωτικότητας και να λάβουν τα αντίστοιχα μέτρα.

Χρήση λογισμικού τρίτων:

Οι περισσότερες mobile εφαρμογές αναπτύσσονται συνδυάζοντας διάφορες λειτουργίες, που αναπτύσσονται από άλλες εταιρείες και όχι από τον προγραμματιστή της εφαρμογής. Αυτές οι βιβλιοθήκες τρίτων μελών βοηθούν τους προγραμματιστές στο: Να παρακολουθούν την δέσμευση των χρηστών (engagement analytics), να συνδέονται στα κοινωνικά δίκτυα και να δημιουργούν έσοδα από την προβολή διαφημίσεων. Ωστόσο, επιπρόσθετα με τις παρεχόμενες υπηρεσίες, οι βιβλιοθήκες μπορούν επίσης να συλλέγουν προσωπικά δεδομένα για δική τους χρήση. Οι ιδιοκτήτες των βιβλιοθηκών μπορούν να χρησιμοποιήσουν αυτήν την πληροφορία για να δημιουργήσουν λεπτομερή ψηφιακά προφίλ των χρηστών, συνδυάζοντας τα δεδομένα που συλλέγουν από διαφορετικές mobile εφαρμογές. Για παράδειγμα, ένας χρήστης μπορεί να δώσει

άδεια σε μία εφαρμογή να συλλέξει την τοποθεσία του/της και μία άλλη εφαρμογή να έχει πρόσβαση στις επαφές του/της. Εάν και οι δύο εφαρμογές χρησιμοποιούν την ίδια βιβλιοθήκη τρίτου μέλους, ο προγραμματιστής της βιβλιοθήκης θα μπορούσε να συνδέσει τα δύο αυτά κομμάτια δεδομένων μαζί. Επιπλέον, οι βιβλιοθήκες αυτές είναι συνήθως ιδιόκτητες και κλειστού κώδικα (closed-source) και δεν μπορούν να αναλυθούν εύκολα. Αυτό έχει ως αποτέλεσμα να είναι συνηθισμένο για ένα προγραμματιστή mobile εφαρμογών να μην κατανοεί πλήρως τι δεδομένα ακριβώς συλλέγουν αυτές οι υπηρεσίες [31]. Αν και αυτό από μόνο του δεν αποτελεί κίνδυνο για την Ασφάλεια, ο συνδυασμός των πηγών των δεδομένων μπορεί να προετοιμάσει το έδαφος για μία επίθεση.

Αγορά εφαρμογών:

Οι εφαρμογές συχνά διανέμονται μέσω συγκεκριμένων ηλεκτρονικών καταστημάτων (app stores), τα οποία μπορούν να διαδραματίσουν σημαντικό ρόλο στην Ασφάλεια και την Ιδιωτικότητα των εφαρμογών. Ένα κατάστημα εφαρμογών συνήθως δεν παρέχει απλά πρόσβαση στις εφαρμογές, αλλά παρέχει πληροφορίες για εφαρμογές, συλλέγει και εμφανίζει αξιολογήσεις χρηστών. Ακόμη, ένα κατάστημα εφαρμογών μπορεί να πραγματοποιεί ελέγχους ασφάλειας σε κάθε παρεχόμενη εφαρμογή, με σκοπό να εμποδίσει την διανομή κακόβουλων ή ψεύτικων εφαρμογών. Λόγω του σημαντικού τους ρόλου για την διανομή των εφαρμογών, οι πάροχοι των καταστημάτων εφαρμογών θα μπορούσαν (ή βάσει κυβερνητικών αιτημάτων, θα αναγκάζονταν) να φιλτράρουν τις εφαρμογές, με γνώμονα τους πιθανούς κινδύνους ασφάλειας, ωστόσο η πολιτική του φιλτραρίσματος θα μπορούσε να βασίζεται σε λόγους αγοράς, πολιτικής ή άλλους. Όσο ο τομέας των καταστημάτων λειτουργεί άναρχα, η πρόσβαση στις δυνατότητες διανομής από προμηθευτές και προγραμματιστές εφαρμογών θα παραμείνει αόριστη και τα κριτήρια για το αν μία εφαρμογή πληροί τις προδιαγραφές ενδέχεται να παραμείνουν αδιαφανή. Η διαθεσιμότητα των εφαρμογών στα αντίστοιχα καταστήματα, καθώς και ο τρόπος παρουσίασής τους μπορεί να επηρεάσει την διανομή των εφαρμογών.

Επιπλέον, από την οπτική γωνία της ιδιωτικότητας, πρέπει να σημειωθεί ότι το γνωστικό επίπεδο της επιλογής των χρηστών μιας εφαρμογής θα μπορούσε να αποτελεί προσωπικό δεδομένο ή ακόμη και ευαίσθητο προσωπικό δεδομένο μερικές φορές(π.χ. εάν εγκατασταθεί μία εφαρμογή e-health, αποκαλύπτονται, ως εκ τούτου, προσωπικές προτιμήσεις ή δεδομένα υγείας). Επί του παρόντος, οι χρήστες ενδέχεται να μην είναι επαρκώς ενημερωμένοι και ανά πάσα στιγμή γνώστες, για την πιθανή συλλογή προσωπικών δεδομένων από τους διαχειριστές ή τους παρόχους του καταστήματος εφαρμογών για την προστιθέμενη αξία των υπηρεσιών που χρησιμοποιούν, εκθέτοντας έτσι τους εαυτούς τους σε κινδύνους κυβερνοασφάλειας.

Αποθήκευση στο «σύννεφο» (cloud):

Οι mobile εφαρμογές συχνά αποθηκεύουν πληροφορίες στο cloud. Αυτή η υπηρεσία θα πρέπει να είναι ασφαλής και θα πρέπει να προστατεύει από διαρροές δεδομένων. Στην πραγματικότητα, έχει αποδειχθεί ότι οι περισσότερες εφαρμογές αποθηκεύουν τα δεδομένα των χρηστών αποκλειστικά στο cloud [11]. Αυτό δημιουργεί μία καινούργια πηγή κινδύνου και απαιτεί από τον χρήστη να εμπιστεύεται τον πάροχο της υπηρεσίας, χωρίς να λαμβάνει υπόψη αντικειμενικά κριτήρια, πάνω στα οποία μπορεί να βασιστεί μία απόφαση εμπιστοσύνης.

Κοινωνικά δίκτυα online:

Πολλές εφαρμογές δίνουν σε έναν χρήστη την επιλογή να μοιραστεί τα δεδομένα του/της (συγκεντρωτικά ή όχι) με άλλους (επιλεγμένους) χρήστες, για λόγους σύγκρισης ή στατιστικής (π.χ. σε ένα κοινωνικό δίκτυο). Αυτό το χαρακτηριστικό επιφέρει τον κίνδυνο διαρροής προσωπικών δεδομένων σε άλλους χρήστες και εισάγει νέους κινδύνους όσον αφορά την Ασφάλεια και την Ιδιωτικότητα, που πρέπει να ληφθούν υπόψη.

Κεφάλαιο 5
Ανάλυση Εφαρμογών m-Health

Στο κεφάλαιο που ακολουθεί θα παρουσιαστεί η μελέτη που πραγματοποιήθηκε σε m-Health εφαρμογές, προκειμένου να διαπιστωθεί ο βαθμός προστασίας των Δεδομένων Προσωπικού Χαρακτήρα των χρηστών, υπό το πρίσμα και του νέου νομικού πλαισίου για την προστασία προσωπικών δεδομένων. Αρχικά θα γίνει μία αναφορά στα κριτήρια επιλογής των m-Health εφαρμογών, καθώς και της μεθοδολογίας που ακολουθήθηκε και κατόπιν θα περιγραφούν τα βήματα μελέτης της κάθε εφαρμογής.

5.1 Κριτήρια επιλογής - Μεθοδολογία

Μετά από αρκετή έρευνα στο διαδίκτυο για τις εφαρμογές m-Health, εστιάσαμε σε «έξυπνες» εφαρμογές ηλεκτρονικής υγείας που έχουν κοινό αντικείμενο. Συγκεκριμένα, σε αυτές που προορίζονται για άτομα που πάσχουν από Σακχαρώδη Διαβήτη (τύπου 1 και 2). Κομβικό σημείο για την απόφαση αυτή είναι ότι ο Σακχαρώδης Διαβήτης αποτελεί σήμερα μείζον πρόβλημα υγείας στον δυτικό κόσμο, ώστε να θεωρείται πανδημία[50]. Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (Π.Ο.Υ.), 171 εκατομμύρια άνθρωποι ή αλλιώς το 2,8% του παγκόσμιου πληθυσμού παρουσιάζει Σακχαρώδη Διαβήτη και υπολογίζεται πως μέχρι το 2030 το ποσοστό αυτό θα έχει σχεδόν διπλασιαστεί.

Όλοι οι τύποι Διαβήτη είναι θεραπεύσιμοι αλλά η θεραπεία για τους τύπους 1 και 2 διαρκούν ολόκληρη τη ζωή. Ο ασθενής λαμβάνει συχνά ινσουλίνη. Η θεραπεία για τους ασθενείς με Διαβήτη τύπου 1 είναι ενέσιμη ινσουλίνη σε συνδυασμό με δίαιτα και άσκηση. Οι ασθενείς με Διαβήτη τύπου 2 συνήθως λαμβάνουν χάπια σε συνδυασμό με δίαιτα και άσκηση, αλλά ανάλογα με την ανταπόκριση κάποιες φορές χρειάζεται να λάβουν ινσουλίνη σε ενέσιμη μορφή.

Όπως καταλαβαίνουμε από τα παραπάνω, τα άτομα που πάσχουν από Σακχαρώδη Διαβήτη πρέπει να μάθουν να ζουν με αυτόν. Η διατήρηση μίας συγκεκριμένης καθημερινής ρουτίνας και η συνεχής παρακολούθηση των επιπέδων ινσουλίνης είναι πολύ σημαντικά. Για το λόγο αυτό,

έχει αναπτυχθεί πληθώρα εφαρμογών m-Health που στόχο έχουν να βοηθήσουν τους πάσχοντες από Σακχαρώδη Διαβήτη στην καθημερινότητά τους. Πρόκειται για εφαρμογές που επιτρέπουν στον χρήστη να εισάγει δεδομένα σχετικά με την πάθησή του και να τα διαχειρίζεται κατάλληλα, ώστε να έχει συγκεντρωμένη όλη την απαραίτητη πληροφορία (π.χ. μετρήσεις σακχάρου, δόσεις ινσουλίνης, δοσολογία φαρμάκων, θερμιδομέτρηση, υπενθυμίσεις μετρήσεων ή λήψης φαρμάκων, κοκ), για να έχει μία – όσο το δυνατόν – πιο φυσιολογική καθημερινότητα.

Επιλέχθηκαν λοιπόν 12 εφαρμογές m-Health με αντικείμενο τον Σακχαρώδη Διαβήτη, οι οποίες:
-Εγκαθίστανται σε λειτουργικό σύστημα Android
-Διατίθενται δωρεάν στο Google Play Store
-Η βαθμολογία τους είναι 4 και άνω (βαθμολογία χρηστών από το Google Play Store)
-Προέρχονται από χώρες τις ΕΕ και τις Η.Π.Α
-Είχαν διαφορετικό αριθμό λήψεων (οι μισές περίπου είχαν πάνω από 100.000 και οι υπόλοιπες ήταν λιγότερο δημοφιλείς)

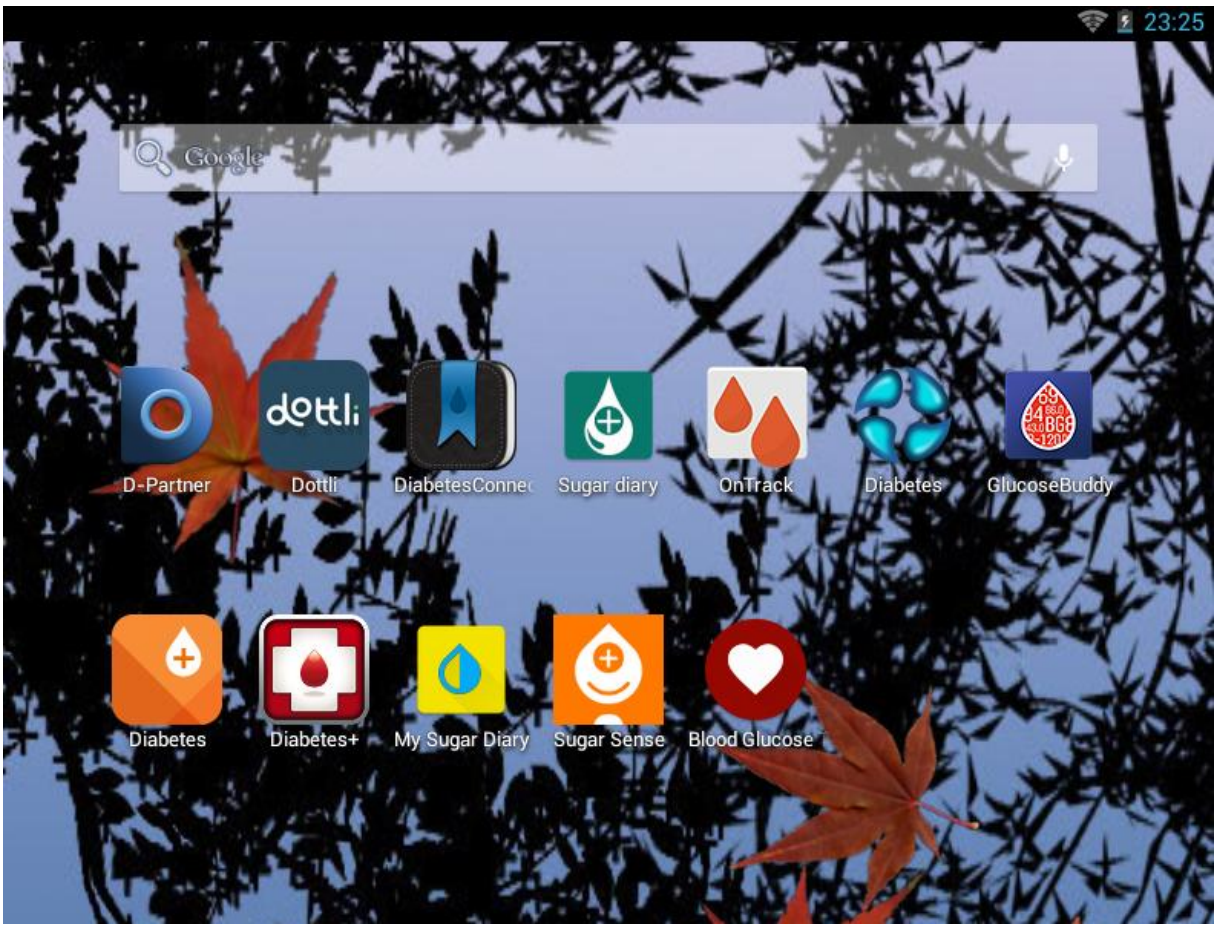
Για την μελέτη των εφαρμογών αυτών εργαστήκαμε ως ακολούθως:
-Δημιουργήσαμε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου (email), για τους σκοπούς της παρούσας έρευνας, με την ονομασία:

-testing.form17@gmail.com

προκειμένου να χρησιμοποιηθεί σε όσες εφαρμογές ζητούσαν την δημιουργία λογαριασμού χρήστη.

-Οι εφαρμογές που επιλέχθηκαν, σύμφωνα με τα παραπάνω κριτήρια, εγκαταστάθηκαν σε συσκευή tablet με τα ακόλουθα τεχνικά χαρακτηριστικά:

-Μάρκα: Bitmore
-Μοντέλο: Tab1022Q
-Android Version: 4.2.2
-Kernel Version: 3.0.36+
-Processor: Cortex A9 Quad Core 1.6 GHz
-RAM: 2 GB
-Storage: 16 GB flash built-in, micro SD card slot (max. 32GB)
-Networking: IEEE 802.11 b/g/n/, Bluetooth



Εικόνα 5.1: Οι m-Health εφαρμογές που εγκαταστάθηκαν στην συσκευή tablet.

- Ακολούθησε στατική ανάλυση των εφαρμογών αυτών. Δηλαδή:

  - Μελετήσαμε τους Όρους Χρήσης (Terms of Use ή Terms of Service ή Service Agreement), την Πολιτική Ασφάλειας (Security Policy ή Security Statement), την Πολιτική Απορρήτου/Ιδιωτικότητας (Privacy Policy ή Privacy Statement), τους Όρους και Προϋποθέσεις (Terms and Conditions), την Νομική Ενημέρωση (Legal Notice), όπου αυτά ήταν διαθέσιμα.

  -Πλοηγηθήκαμε στις εφαρμογές αυτές, προκειμένου να εντοπίσουμε τυχόν ζητήματα ασφάλειας όπως: Διαχείριση cookies, σύνδεση https (δηλ. κρυπτογραφημένη σύνδεση), υπηρεσίες τρίτων μερών (third-parties), διαφημίσεις, κτλ.

Όλα τα παραπάνω έγιναν για να διαπιστωθεί η συμμόρφωση ή μη των συγκεκριμένων m-Health εφαρμογών με τις απαιτήσεις τις ισχύουσας νομοθεσίας, για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα και ιδιαιτέρως με τον ΓΚΠΔ, μιας και η τελική ημερομηνία υποχρέωσης συμμόρφωσης με τις διατάξεις του είναι η 25η Μαΐου 2018, δηλαδή λίγες μόνο ημέρες μετά το πέρας συγγραφής της παρούσας μεταπτυχιακής διατριβής.

Επιγραμματικά, τα σημεία εκείνα στα οποία εστιάσαμε την μελέτη μας είναι:

1. Προαπαιτούμενες πληροφορίες χρήστη για την εγκατάσταση των εφαρμογών

2. Το Δικαίωμα της Ενημέρωσης

3. Το Δικαίωμα της Πρόσβασης

4. Το Δικαίωμα της Διόρθωσης

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας

6. Το Δικαίωμα στη Λήθη/της Διαγραφής

7. Το Δικαίωμα στην Φορητότητα των Δεδομένων

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του

10. Αρχή της Αναλογικότητας

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση)

12. Γονική Συναίνεση

Από τα παραπάνω, το Δικαίωμα Περιορισμού της Επεξεργασίας, το Δικαίωμα στη Λήθη/της Διαγραφής, το Δικαίωμα στην Φορητότητα των Δεδομένων και το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων, είναι απαιτήσεις που συναντούμε για πρώτη φορά στον ΓΚΠΔ, του οποίου – όπως αναφέραμε και προηγουμένως - η τελική ημερομηνία υποχρέωσης συμμόρφωσης με τις διατάξεις του είναι η 25η Μαΐου 2018, δηλαδή λίγες ημέρες μετά την ολοκλήρωση της μελέτης μας.

Με βάση όλα τα παραπάνω, θα προσπαθήσουμε να απαντήσουμε στα ακόλουθα ερευνητικά ερωτήματα:

H1: Είναι η επεξεργασία προσωπικών δεδομένων σύμφωνη με τις βασικές προϋποθέσεις νομιμότητας του ΓΚΠΔ;

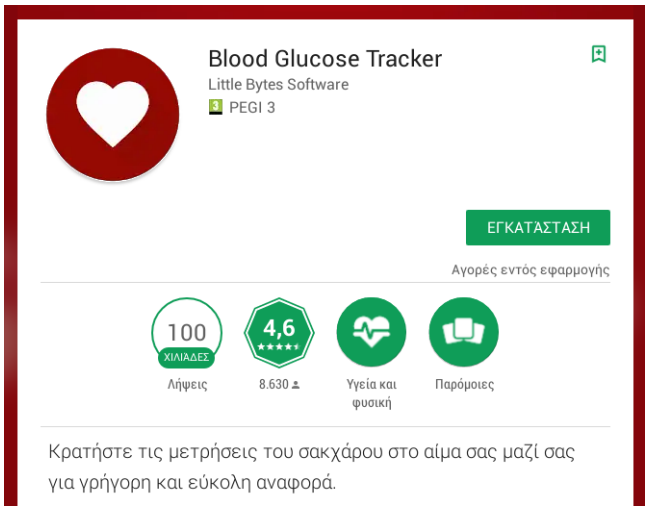
H2: Ικανοποιούνται τα δικαιώματα των χρηστών που προβλέπονται στον ΓΚΔΠ;

H3: Είναι η επεξεργασία ασφαλής;

Ακολουθεί η παρουσίαση των επιλεγέντων m-Health εφαρμογών κατά αλφαβητική σειρά. Έγινε προσπάθεια κατηγοριοποίησης των κριτηρίων, με βάσει όσα αναφέραμε στα προηγούμενα κεφάλαια για την νομοθεσία περί προστασίας των Δεδομένων Προσωπικού Χαρακτήρα, για να είμαστε σε θέση να ποσοτικοποιήσουμε - κατά κάποιον τρόπο – τα αποτελέσματα, ώστε να

παρουσιαστούν στο επόμενο κεφάλαιο με σαφήνεια, ακρίβεια και απλότητα και να γίνουν κατανοητά από όλους.

5.2 Blood Glucose Tracker Application



Εικόνα 5.2: Blood Glucose Tracker Application [5]

Από την ανάλυση της εφαρμογής, προέκυψαν τα ακόλουθα στοιχεία:

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Ταυτότητα.

2. Το Δικαίωμα της Ενημέρωσης: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) είναι αρκετά αναλυτικές.

3. Το Δικαίωμα της Πρόσβασης: Η εφαρμογή δίνει την δυνατότητα στον χρήστη να κάνει backup των τοπικών του αρχείων. Τα δεδομένα που αποθηκεύονται στην συσκευή είναι υπό τον πλήρη έλεγχό του. Επίσης, δίνεται στον χρήστη η δυνατότητα να ζητήσει πληροφορίες για τα δεδομένα που αποθηκεύει κεντρικά η εφαρμογή (π.χ. σε servers του κατασκευαστή της εφαρμογής, σε cloud, κτλ) και αφορούν το πρόσωπό του.

4. Το Δικαίωμα της Διόρθωσης: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται σχετική διαδικασία, παρά το γεγονός ότι υπάρχει η δυνατότητα πρόσβασης στα

δεδομένα που αποθηκεύει κεντρικά η εφαρμογή (π.χ. σε servers του κατασκευαστή της εφαρμογής, σε cloud, κτλ), μετά από αίτηση του χρήστη.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται σχετική διαδικασία. Αναφέρεται μόνον ότι γίνεται επεξεργασία μη-ταυτοποιήσιμων πληροφοριών, σαν αυτές που χρησιμοποιεί συνήθως η υπηρεσία Google Analytics, όπως το λειτουργικό σύστημα, ο κατασκευαστής της συσκευής και η – κατά προσέγγιση – τοποθεσία του χρήστη. Πουθενά όμως δεν αναφέρεται εάν ο χρήστης μπορεί να ζητήσει τον περιορισμό της επεξεργασίας των δεδομένων αυτών.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο χρήστης δύναται ανά πάσα στιγμή να απεγκαταστήσει την εφαρμογή από την συσκευή του. Επίσης μπορεί να ζητήσει να διαγραφούν τα δεδομένα που αποθηκεύει κεντρικά η εφαρμογή (π.χ. σε servers του κατασκευαστή της εφαρμογής, σε cloud, κτλ). Η ακριβής έκφραση που χρησιμοποιείται είναι: «Θα καταργήσουμε αυτά τα δεδομένα στο μέτρο που επιτρέπεται από το νόμο».

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Ο χρήστης έχει την δυνατότητα να εξάγει τα αρχεία του (file export), αλλά δεν διευκρινίζεται εάν τα αρχεία αυτά θα μπορούν να χρησιμοποιηθούν σε άλλη εφαρμογή.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται σχετική διαδικασία.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) είναι αρκετά αναλυτικές. Δεν υποχρεώνεται όμως ο χρήστης, ούτε προτρέπεται με κάποιον τρόπο να τις διαβάσει. Για παράδειγμα, δεν υπάρχει check-box στο οποίο ο χρήστης να έχει την δυνατότητα να επιλέξει π.χ: «Με την εγκατάσταση συναινώ στην περιγραφείσα επεξεργασία δεδομένων».

10. Αρχή της Αναλογικότητας: Τα δεδομένα που εισάγει ο χρήστης είναι όλα σχετικά με το προφίλ του και την κατάσταση της υγείας του. Φαινομενικά, δεν υπάρχουν υποχρεωτικά – προς συμπλήρωση πεδία – τα οποία να μην έχουν σχέση με τους σκοπούς της εφαρμογής ή να

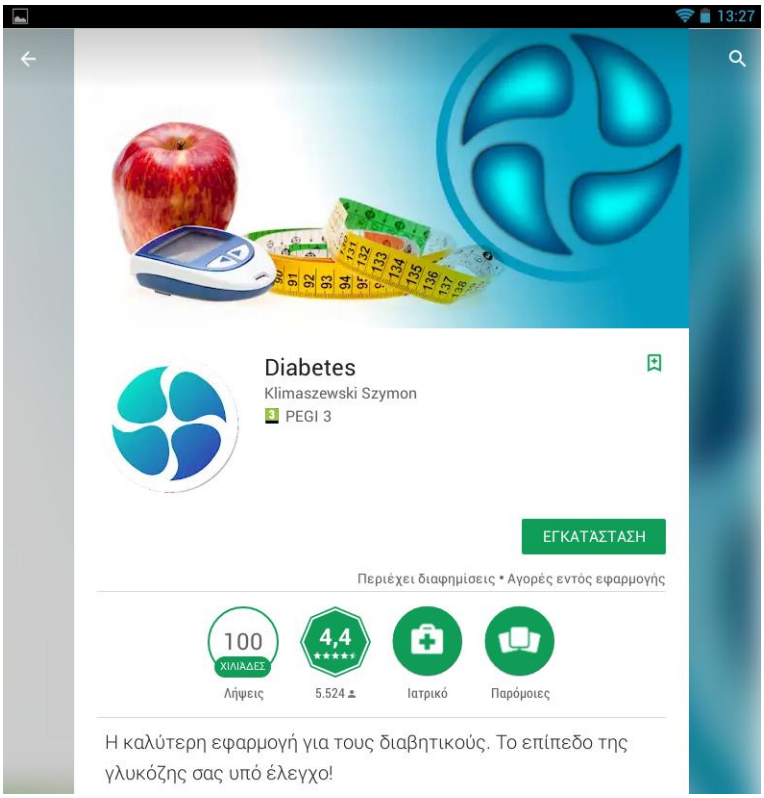
μην σχετίζονται με την εκτέλεση κάποιας από τις υπηρεσίες που παρέχει στους χρήστες. Η εφαρμογή φαίνεται να πληροί το κριτήριο αυτό.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Γίνεται εκτενής αναφορά στις βιβλιοθήκες ανοικτού κώδικα που χρησιμοποιεί η εφαρμογή (Open Source Info). Κάποιες από αυτές χρησιμοποιούν σύνδεση https (6), ενώ κάποιες άλλες όχι(4).

12. Γονική Συναίνεση: Η Νομική Ενημέρωση (Legal Notice) και η Δήλωση Ιδιωτικότητας/Απορρήτου (Privacy Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται σχετική διαδικασία. Επιπλέον, δεν αναφέρει πουθενά ότι αυτή η εφαρμογή απευθύνεται σε ηλικίες άνω των 16 ή άνω των 18 και δεν υπάρχει καν ένα check-box στο οποίο ο χρήστης να έχει την δυνατότητα να δηλώσει την ηλικία του.

Παρατήρηση: Γνωστοποιείται στους χρήστες εκτός Η.Π.Α. ότι οι ταυτοποιήσιμες πληροφορίες (ταυτότητα) για το πρόσωπό τους (που συγχρονίζουν στην συσκευή τους), θα μεταφέρονται από την χώρα τους στις Η.Π.Α. και άλλες χώρες, χωρίς να διευκρινίζονται οι χώρες αυτές. Επί λέξει, το σχετικό κείμενο αναφέρει: *"...any personally identifiable information you synchronize will be transferred out of your country and into the United States and possibly to other countries. By using the application you consent to such transfer..."* . Δεν υποχρεώνεται όμως ο χρήστης, ούτε προτρέπεται με κάποιον τρόπο να διαβάσει την συγκεκριμένη δήλωση απορρήτου. Για παράδειγμα, δεν υπάρχει check-box στο οποίο ο χρήστης να έχει την δυνατότητα να επιλέξει π.χ: «Με την εγκατάσταση συναινώ στην περιγραφείσα επεξεργασία δεδομένων».

5.3 Diabetes Application



Εικόνα 5.3: Diabetes Application [13]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Φωτογραφίες/Μέσα/Αρχεία .

2. Το Δικαίωμα της Ενημέρωσης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Η απουσία αυτή, συνεπάγεται άγνοια του χρήστη για τον εάν η συγκεκριμένη εφαρμογή πληροί τις απαιτήσεις της σχετικής νομοθεσίας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

3. Το Δικαίωμα της Πρόσβασης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Η απουσία αυτή, συνεπάγεται άγνοια του χρήστη για το εάν η συγκεκριμένη εφαρμογή πληροί τις απαιτήσεις της σχετικής νομοθεσίας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

4. Το Δικαίωμα της Διόρθωσης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Η

απουσία αυτή, συνεπάγεται άγνοια του χρήστη για τον εάν η συγκεκριμένη εφαρμογή πληροί τις απαιτήσεις της σχετικής νομοθεσίας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Υπάρχει μόνο ένα check-box για την επιλογή Google Analytics (Collects anonymous data about application usage), με το οποίο ο χρήστης μπορεί να ενεργοποιήσει ή όχι την επιλογή αυτή.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο χρήστης έχει την δυνατότητα να διαγράψει (τοπικά στην συσκευή του) όλες τις πληροφορίες που έχει εισάγει μέχρι την στιγμή εκείνη. Δεν παρέχεται ειδική ενημέρωση για το αν τα δεδομένα του χρήστη αποθηκεύονται σε server της εταιρείας.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Ο χρήστης έχει την δυνατότητα να εξάγει τα αρχεία του (export data), και να τα αποστείλει είτε σε email, είτε σε εξωτερική μνήμη. Επίσης, μπορεί να τα εξάγει είτε σε μορφή αναφοράς, είτε σε απλά δεδομένα (raw data), αλλά δεν διευκρινίζεται εάν τα αρχεία αυτά θα μπορούν να χρησιμοποιηθούν σε άλλη εφαρμογή.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Η απουσία αυτή, συνεπάγεται άγνοια του χρήστη για τον εάν η συγκεκριμένη εφαρμογή πληροί τις απαιτήσεις της σχετικής νομοθεσίας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Η απουσία αυτή, συνεπάγεται άγνοια του χρήστη για τον εάν η συγκεκριμένη εφαρμογή πληροί τις απαιτήσεις της σχετικής νομοθεσίας για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα.

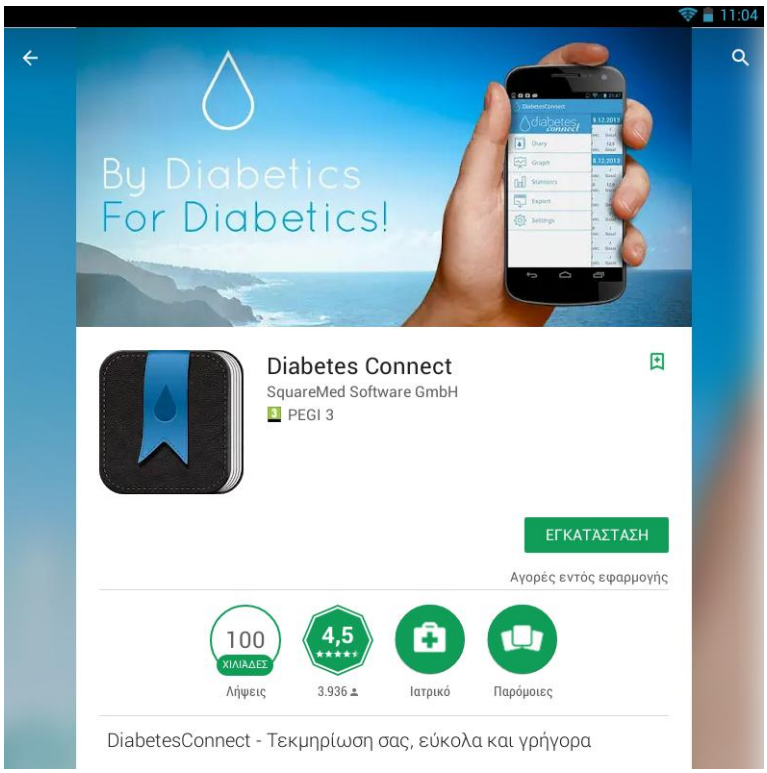
10. Αρχή της Αναλογικότητας: Οι πληροφορίες που ζητά η εφαρμογή από τον χρήστη είναι οι απολύτως απαραίτητες για την εξυπηρέτηση των σκοπών της εφαρμογής. Η εφαρμογή φαίνεται, εκ πρώτης όψεως, να πληροί το κριτήριο αυτό.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Δεν κατέστη δυνατή η εξακρίβωση ύπαρξης ή μη κάποιας συγκεκριμένης μορφής κρυπτογράφησης.

12. Γονική Συναίνεση: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Δεν καταφέραμε να εντοπίσουμε κάποιο σημείο όπου να αναφέρεται ότι αυτή η εφαρμογή απευθύνεται σε ηλικίες άνω των 16 ή άνω των 18 και δεν υπάρχει καν ένα check-box στο οποίο ο χρήστης να έχει την δυνατότητα να δηλώσει την ηλικία του.

Παρατήρηση: Η εφαρμογή καλεί τον χρήστη να καταβάλλει ένα ποσό εφάπαξ, προκειμένου να απαλλαγεί από τις διαφημίσεις, οι οποίες είναι αρκετά ενοχλητικές. Βέβαια, στην οθόνη λήψης της εφαρμογής (Εικόνα 5.3) υπάρχει ενημέρωση ότι περιέχονται διαφημίσεις, επομένως η απόφαση: Εγκατάσταση ή όχι και Πληρωμή ή όχι, είναι αποκλειστική ευθύνη του χρήστη.

5.4 Diabetes Connect Application



Εικόνα 5.4: Diabetes Connect Application [14]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Φωτογραφίες/Μέσα/Αρχεία.

2. Το Δικαίωμα της Ενημέρωσης: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "*404 Not Found - The requested URL was not found on this server*". Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να γνωρίζει αν η εν λόγω εφαρμογή υπακούει στις επιταγές τις σχετικής νομοθεσίας.

3. Το Δικαίωμα της Πρόσβασης: Στις συνήθεις ερωτήσεις (Frequently Asked Questions - FAQs) πληροφορούμαστε ότι τα δεδομένα του χρήστη συγχρονίζονται στο παρασκήνιο με τους servers της εφαρμογής, αρκεί να υπάρχει διαθέσιμη μία έγκυρη σύνδεση στο διαδίκτυο. Έτσι, ακόμη και εάν η συσκευή του χρήστη χαλάσει ή χαθεί, τα δεδομένα του είναι ακόμη διαθέσιμα. Ο χρήστης μπορεί να αποκτήσει πρόσβαση σε αυτά κάνοντας login είτε από τη νέα του συσκευή, είτε στο web portal: https://portal.diabetesconnect.de

4. Το Δικαίωμα της Διόρθωσης: Στις συνήθεις ερωτήσεις (Frequently Asked Questions - FAQs) πληροφορούμαστε ότι τα δεδομένα του χρήστη συγχρονίζονται στο παρασκήνιο με τους servers της εφαρμογής, αρκεί να υπάρχει διαθέσιμη μία έγκυρη σύνδεση στο διαδίκτυο. Έτσι, ακόμη και εάν η συσκευή του χρήστη χαλάσει ή χαθεί, τα δεδομένα του είναι ακόμη διαθέσιμα. Ο χρήστης μπορεί να αποκτήσει πρόσβαση σε αυτά κάνοντας login είτε από τη νέα του συσκευή, είτε στο web portal: https://portal.diabetesconnect.de

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "404 Not Found - The requested URL was not found on this server". Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να γνωρίζει αν η εν λόγω εφαρμογή υπακούει στις επιταγές τις σχετικής νομοθεσίας.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "404 Not Found - The requested URL was not found on this server". Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να γνωρίζει αν η εν λόγω εφαρμογή υπακούει στις επιταγές τις σχετικής νομοθεσίας.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Ο χρήστης έχει την δυνατότητα να εξάγει τα αρχεία του σε μορφή pdf, το οποίο δεν φαίνεται να είναι σύμφωνο με τις απαιτήσεις του δικαιώματος φορητότητας του ΓΚΠΔ, αφού το .pdf δεν αποτελεί μορφότυπο που μπορεί να

επιτρέψει σε μία άλλη εφαρμογή την ευχερή εισαγωγή των δεδομένων στο πλαίσιο ικανοποίησης του δικαιώματος στη φορητότητα.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "*404 Not Found - The requested URL was not found on this server*". Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να γνωρίζει αν η εν λόγω εφαρμογή υπακούει στις επιταγές τις σχετικής νομοθεσίας.

9 . Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "*404 Not Found - The requested URL was not found on this server*". Αυτό σημαίνει ότι ο χρήστης δεν μπορεί να γνωρίζει αν η εν λόγω εφαρμογή υπακούει στις επιταγές τις σχετικής νομοθεσίας.

10. Αρχή της Αναλογικότητας: Οι εφαρμογή κατά την πρώτη της εκκίνηση ζητά από τον χρήστη πληροφορίες προκειμένου να κάνει μία αρχική παραμετροποίηση (configuration). Όλες οι πληροφορίες αυτές (π.χ. φύλο, βάρος, τύπος διαβήτη, κτλ) είναι απολύτως σχετικές με την λειτουργία της εφαρμογής. Επομένως, η εφαρμογή φαίνεται κατ' αρχάς ότι ικανοποιεί την Αρχή της αναλογικότητας.

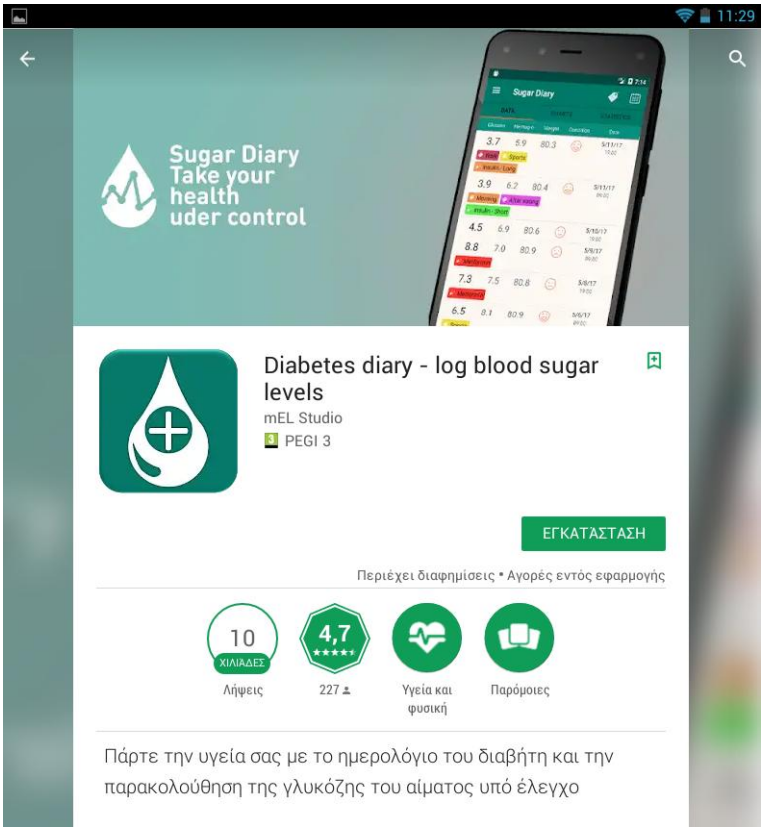
11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Στις συνήθεις ερωτήσεις (Frequently Asked Questions - FAQs) πληροφορούμαστε ότι τα δεδομένα του χρήστη συγχρονίζονται στο παρασκήνιο με τους servers της εφαρμογής, αρκεί να υπάρχει διαθέσιμη μία έγκυρη σύνδεση στο διαδίκτυο. Έτσι, ακόμη και εάν η συσκευή του χρήστη χαλάσει ή χαθεί, τα δεδομένα του είναι ακόμη διαθέσιμα. Ο χρήστης μπορεί να αποκτήσει πρόσβαση σε αυτά κάνοντας login είτε από τη νέα του συσκευή, είτε στο web portal: https://portal.diabetesconnect.de. Επομένως, μπορούμε να πούμε ότι υπάρχει κρυπτογραφημένη σύνδεση με τον web server.

12. Γονική Συναίνεση: Ο σύνδεσμος (link) στην εφαρμογή που παραπέμπει στην Πολιτική Απορρήτου (Privacy Policy) δείχνει να μην λειτουργεί. Στην προσπάθειά μας να συνδεθούμε εμφάνιζε το μήνυμα σφάλματος: "*404 Not Found - The requested URL was not found on this server*". Πέραν τούτου, δεν καταφέραμε να εντοπίσουμε κάποιο σημείο όπου να

αναφέρεται ότι αυτή η εφαρμογή απευθύνεται σε ηλικίες άνω των 16 ή άνω των 18 και δεν υπάρχει κάποιο πεδίο στο οποίο ο χρήστης να καλείται να δηλώσει την ηλικία του.

Παρατήρηση: Απαιτείται η δημιουργία Λογαριασμού Χρήστη, του οποίου ο Κωδικός Πρόσβασης πρέπει να έχει ελάχιστο μήκος 6 χαρακτήρες και να περιέχει τουλάχιστον ένα γράμμα και έναν αριθμό.

5.5 Diabetes Diary Application



Εικόνα 5.5: Diabetes Diary Application [15]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Τοποθεσία, Φωτογραφίες/Μέσα/Αρχεία, Πληροφορίες σύνδεσης Wi-Fi.

2. Το Δικαίωμα της Ενημέρωσης: Η Πολιτική Απορρήτου (Privacy Policy) αναφέρει αρκετές πληροφορίες με απλό και σαφή τρόπο.

3. Το Δικαίωμα της Πρόσβασης: Η Πολιτική Απορρήτου (Privacy Policy) δεν αναφέρει κάτι σχετικό, ούτε καταφέραμε να εντοπίσουμε σε κάποιο άλλο σημείο της εφαρμογής την

περιγραφή κάποιας σχετικής διαδικασίας, αλλά ούτε και κάποιο check-box που να απευθύνεται στον χρήστη. Υπάρχει πάντως διαθέσιμο το email: mmelstudio@gmail.com για επικοινωνία του χρήστη με την εταιρεία, για οποιοδήποτε -σχετικό με την Πολιτική Απορρήτου - θέμα μπορεί να τον απασχολεί.

4. Το Δικαίωμα της Διόρθωσης: Η Πολιτική Απορρήτου (Privacy Policy) δεν αναφέρει κάτι σχετικό, ούτε καταφέραμε να εντοπίσουμε σε κάποιο άλλο σημείο της εφαρμογής την περιγραφή κάποιας σχετικής διαδικασίας, αλλά ούτε και κάποιο check-box που να απευθύνεται στον χρήστη. Υπάρχει πάντως διαθέσιμο το email: mmelstudio@gmail.com για επικοινωνία του χρήστη με την εταιρεία, για οποιοδήποτε -σχετικό με την Πολιτική Απορρήτου - θέμα μπορεί να τον απασχολεί.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Η Πολιτική Απορρήτου (Privacy Policy) δεν αναφέρει κάτι σχετικό, ούτε καταφέραμε να εντοπίσουμε σε κάποιο άλλο σημείο της εφαρμογής την περιγραφή κάποιας σχετικής διαδικασίας, αλλά ούτε και κάποιο check-boxπου να απευθύνεται στον χρήστη. Υπάρχει πάντως διαθέσιμο το email:mmelstudio@gmail.comγια επικοινωνία του χρήστη με την εταιρεία, για οποιοδήποτε -σχετικό με την Πολιτική Απορρήτου - θέμα μπορεί να τον απασχολεί.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο χρήστης έχει την δυνατότητα να διαγράψει τοπικά τα δεδομένα του με την επιλογή: “Clear data – Delete all records”. Πουθενά όμως δεν αναφέρεται – ούτε περιγράφεται ανάλογη διαδικασία - ότι ο χρήστης έχει το δικαίωμα να ζητήσει την πλήρη διαγραφή των δεδομένων του που βρίσκονται αποθηκευμένα στους servers της εταιρείας.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Η εφαρμογή δίνει την δυνατότητα Backup σε κάρτα μνήμης SD ή στο Google Drive, αλλά δεν διευκρινίζεται εάν τα αρχεία αυτά θα μπορούν να χρησιμοποιηθούν σε άλλη εφαρμογή

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Η Πολιτική Απορρήτου (Privacy Policy) δεν αναφέρει κάτι σχετικό ούτε καταφέραμε να εντοπίσουμε σε κάποιο άλλο σημείο της εφαρμογής την περιγραφή κάποιας σχετικής διαδικασίας, αλλά ούτε και κάποιο check-box που να απευθύνεται στον χρήστη. Υπάρχει πάντως διαθέσιμο το email: mmelstudio@gmail.com για επικοινωνία του χρήστη με την εταιρεία, για οποιοδήποτε -σχετικό με την Πολιτική Απορρήτου - θέμα μπορεί να τον απασχολεί.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Η Πολιτική Απορρήτου (Privacy Policy) είναι αρκετά αναλυτική. Δεν υποχρεώνεται όμως ο χρήστης, ούτε προτρέπεται με κάποιον τρόπο να την διαβάσει, αλλά ούτε και υπάρχει κάποιο check-box στο οποίο ο χρήστης να έχει την δυνατότητα να επιλέξει π.χ: «Με την εγκατάσταση συναινώ στην περιγραφείσα επεξεργασία δεδομένων». Επιπλέον, πέραν της βασικής λειτουργίας της εφαρμογής, στους όρους χρήσης κάνει λόγο για cookies τρίτων ("third-parties code and libraries that use cookies"), τα οποία ο χρήστης μπορεί είτε να δεχθεί, είτε να απορρίψει. Σημειώνεται όμως, ότι σε περίπτωση απόρριψης των cookies αυτών, δεν υπάρχει εγγύηση ότι θα λειτουργούν σωστά όλες οι υπηρεσίες της εφαρμογής.

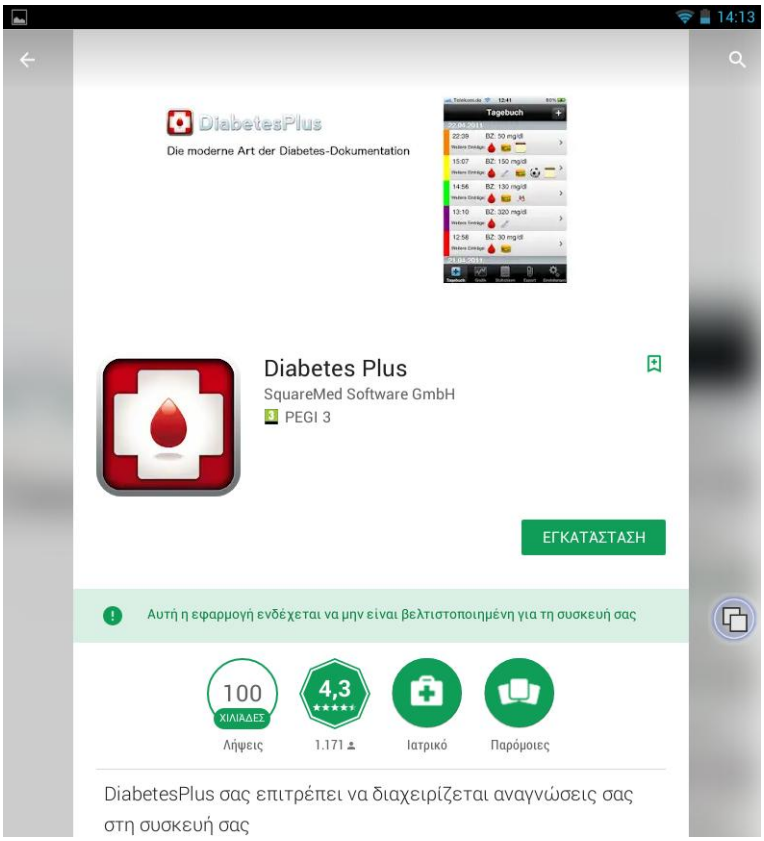
10. Αρχή της Αναλογικότητας: Στην Πολιτική Απορρήτου (Privacy Policy) υπάρχει ειδικό κεφάλαιο που περιγράφει την συλλογή δεδομένων (Information Collection and Use), καθώς και την διευκρίνιση ότι χρησιμοποιούνται μόνο για τους σκοπούς που περιγράφονται σε αυτή. Εξίσου σημαντική είναι η ενημέρωση ότι οι ταυτοποιήσιμες πληροφορίες που ζητούνται παραμένουν στην συσκευή του χρήστη και δεν συλλέγονται από την εταιρεία με κανένα τρόπο. Παρ' όλα αυτά, η εφαρμογή κατά την αρχική της εγκατάσταση ζητά από τον χρήστη πρόσβαση σε πληροφορίες όπως: Τοποθεσία, Φωτογραφίες/Μέσα/Αρχεία, Πληροφορίες σύνδεσης Wi-Fi, οι οποίες δεν σχετίζονται με το αντικείμενό της. Έτσι, μπορούμε να θεωρήσουμε ότι η Αρχή της αναλογικότητας δεν εκπληρούται.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Η σύνδεση με την ιστοσελίδα της εφαρμογής για πρόσβαση στην Πολιτική Απορρήτου είναι: http://melstudio.info/en/privacy-policy, δηλαδή μη κρυπτογραφημένη. Ωστόσο, αναφορικά με τη μεταφορά των δεδομένων από τη συσκευή του χρήστη, εδώ έχουμε μία περίπτωση όπου δεν κατέστη δυνατό να εξακριβωθεί η ύπαρξη ή μη κάποιας συγκεκριμένης τεχνικής κρυπτογράφησης.

12. Γονική Συναίνεση: Στην Πολιτική Απορρήτου (Privacy Policy) αναφέρεται ρητά ότι η εφαρμογή δεν απευθύνεται σε παιδιά κάτω των 13 ετών. Σε περίπτωση που διαπιστωθεί ότι κάποιος χρήστης είναι κάτω των 13 ετών, θα διαγράφεται από τους servers. Δεν διευκρινίζει ωστόσο τον τρόπο εντοπισμού και αποκλεισμού τους. Επιπλέον, προτρέπει τους γονείς, σε περίπτωση που αντιληφθούν ότι το παιδί τους έχει εισάγει προσωπικές του πληροφορίες στην εφαρμογή, να ειδοποιήσουν αμέσως την εταιρεία ώστε να προβεί στις απαραίτητες ενέργειες.

Παρατήρηση:Στην Πολιτική Απορρήτου (Privacy Policy) περιγράφονται αναλυτικά τα permissions που απαιτεί η εφαρμογή από την συσκευή του χρήστη (π.χ camera, storage, log data).

5.6 Diabetes Plus Application



Εικόνα 5.5: Diabetes Plus Application [16]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Φωτογραφίες/Μέσα/Αρχεία.

2. Το Δικαίωμα της Ενημέρωσης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Έτσι ο χρήστης δεν είναι σε θέση να γνωρίζει εάν η εφαρμογή αυτή είναι σύμφωνη με τις σχετικές διατάξεις της ισχύουσας νομοθεσίας.

3. Το Δικαίωμα της Πρόσβασης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Έτσι ο

χρήστης δεν είναι σε θέση να γνωρίζει εάν η εφαρμογή αυτή είναι σε σύμπνοια με τις σχετικές διατάξεις της ισχύουσας νομοθεσίας.

4. Το Δικαίωμα της Διόρθωσης: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Έτσι ο χρήστης δεν είναι σε θέση να γνωρίζει εάν η εφαρμογή αυτή είναι σε σύμπνοια με τις σχετικές διατάξεις της ισχύουσας νομοθεσίας.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Έτσι ο χρήστης δεν είναι σε θέση να γνωρίζει εάν η εφαρμογή αυτή είναι σε σύμπνοια με τις σχετικές διατάξεις της ισχύουσας νομοθεσίας.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Δίνεται στον χρήστη η επιλογή να διαγράψει όλα τα δεδομένα του, με την προειδοποίηση ότι η διαγραφή αυτή είναι μη αναστρέψιμη.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Η εφαρμογή δίνει την δυνατότητα εξαγωγής αρχείου, όπου ο - εκ προεπιλογής - παραλήπτης είναι το email του γιατρού, το οποίο έχει κληθεί προηγουμένως να εισάγει ο χρήστης. Βεβαία, στο σημείο αυτό μπορεί κατ' επέκταση να εισαχθεί οποιοδήποτε έγκυρο email. Υπάρχει και μία επιπλέον επιλογή εξαγωγής δεδομένων απευθείας στην εφαρμογή "Diabetes Connect" που εξετάσαμε στο κεφάλαιο 5.4 και αυτό γιατί ανήκουν στην ίδια εταιρεία: "SuareMed Software GmbH". Με την πληροφορία αυτή όμως δεν μπορούμε να ισχυριστούμε ότι πληροί το δικαίωμα στην φορητότητα.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Έτσι ο χρήστης δεν είναι σε θέση να γνωρίζει εάν η εφαρμογή αυτή είναι σε σύμπνοια με τις σχετικές διατάξεις της ισχύουσας νομοθεσίας.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Δεν υπήρχαν σύνδεσμοι στην εφαρμογή που να παραπέμπουν σε οποιαδήποτε μορφή Όρων Χρήσης ή Πολιτική Ασφάλειας/Απορρήτου. Επομένως και η απουσία κάποιου check-box

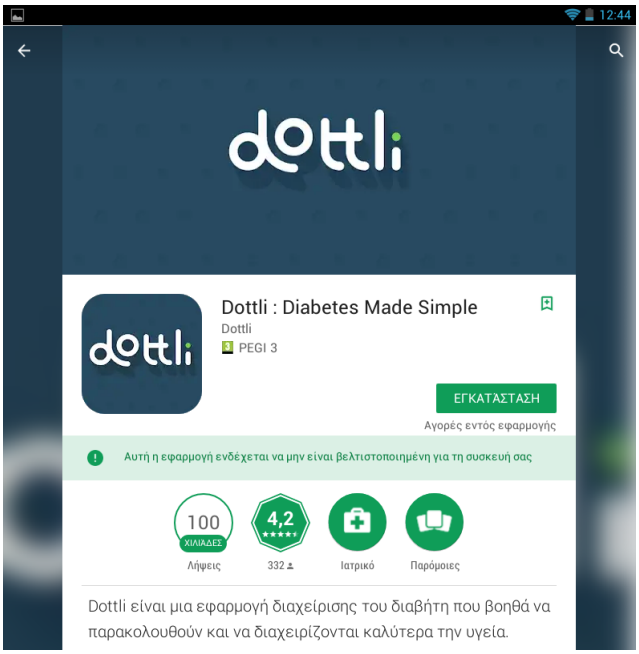
στο οποίο ο χρήστης να έχει την δυνατότητα να επιλέξει π.χ: «Με την εγκατάσταση συναινώ στην περιγραφείσα επεξεργασία δεδομένων» κρίνεται απολύτως λογική.

10. Αρχή της Αναλογικότητας: Οι πληροφορίες (βάρος, τιμές γλυκόζης, τιμές ινσουλίνης, κτλ) που ζητά η εφαρμογή από τον χρήστη είναι απολύτως σχετικές με τους σκοπούς της εφαρμογής για την διαχείριση του Σακχαρώδη Διαβήτη.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Δεν αναφέρεται κάποια σύνδεση με server της εταιρείας, αλλά ούτε και υπάρχει παραπομπή σε κάποια ιστοσελίδα, προκειμένου να εξακριβώσουμε αν τα δεδομένα του χρήστη πηγαίνουν σε server της εταιρείας ή την ύπαρξη κάποιας μορφής κρυπτογράφησης.

12. Γονική Συναίνεση: Η εφαρμογή ζητά την ημερομηνία γέννησης του χρήστη. Βέβαια ο χρήστης μπορεί να εισάγει ότι στοιχεία θέλει, αρκεί να είναι έγκυρα (π.χ. δεν μπορεί να βάλει έτος γέννησης το 1800 ή το 2050), όπως και στην περίπτωση που ζητείται το email ττου γιατρού. Δεν καταφέραμε όμως να εντοπίσουμε κάποια αναφορά ότι – παραδείγματος χάρη - απευθύνεται μόνο σε ενήλικες ή ότι σε περίπτωση ανήλικου χρήστη απαιτείται η γονική συναίνεση.

5.7 Dottli Diabetes Made Simple Application



Εικόνα 5.7: Dottli Diabetes Made Simple Application [17]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Ταυτότητα, Επαφές, Τοποθεσία, Φωτογραφίες/Μέσα/Αρχεία, Πληροφορίες σύνδεσης Wi-Fi, Πληροφορίες σύνδεσης Bluetooth.

2. Το Δικαίωμα της Ενημέρωσης: Οι Όροι Χρήσης (Terms of Use) και η Δήλωση Ασφάλειας (Security Statement) είναι αρκούντως αναλυτικοί και επεξηγηματικοί. Χρησιμοποιούνται ακόμη και παραδείγματα και υποθετικές περιπτώσεις για την καλύτερη κατανόηση των σχετικών όρων. Δίνεται όμως η δυνατότητα στον χρήστη να επιλέξει το κουμπί "Accept" χωρίς να έχει διαβάσει τους Όρους Χρήσης και την Δήλωση Ασφάλειας.

3. Το Δικαίωμα της Πρόσβασης: Ο χρήστης έχει το δικαίωμα - ανά πάσα στιγμή - να ζητήσει ηλεκτρονικό αντίγραφο των δεδομένων του.

4. Το Δικαίωμα της Διόρθωσης: Ο χρήστης μπορεί να ζητήσει την τροποποίηση οποιασδήποτε πληροφορίας, την οποία θεωρεί λανθασμένη ή ελλιπή.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Ο χρήστης έχει τον πλήρη έλεγχο ως προς το με ποιον θα "μοιράζεται" τα δεδομένα του. Στους Όρους Χρήσης αναφέρεται ότι τα δεδομένα των χρηστών μπορούν να δοθούν π.χ. σε συνεργαζόμενες επιχειρήσεις ή σε ερευνητές, αφού πρώτα ζητηθεί έγκριση από τον χρήστη και αφαιρεθούν όλες οι προσωπικές πληροφορίες που θα μπορούσαν να τον ταυτοποιήσουν .

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Οι Όροι Χρήσης (Terms of Use) και η Δήλωση Ασφάλειας (Security Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται ανάλογη διαδικασία.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Ο χρήστης έχει το δικαίωμα να ζητήσει να σταλεί ηλεκτρονικό αντίγραφο των Προστατευόμενων Πληροφοριών του Υγείας (Protected Health Information - PHI) είτε στον ίδιο, είτε σε τρίτο πρόσωπο που αυτός θα ορίσει.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Οι Όροι Χρήσης (Terms of Use) και η Δήλωση Ασφάλειας (Security Statement) δεν αναφέρουν κάτι σχετικό, ούτε περιγράφεται ανάλογη διαδικασία.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Οι Όροι Χρήσης (Terms of Use) και η Δήλωση Ασφάλειας (Security Statement) είναι αρκετά

αναλυτικοί. Στους Όρους Χρήσης αναφέρεται ότι τα δεδομένα των χρηστών μπορεί να δοθούν π.χ. σε συνεργαζόμενες επιχειρήσεις ή σε ερευνητές, αφού πρώτα ζητηθεί έγκριση από τον χρήστη και αφαιρεθούν όλες οι προσωπικές πληροφορίες που θα μπορούσαν να τον ταυτοποιήσουν.

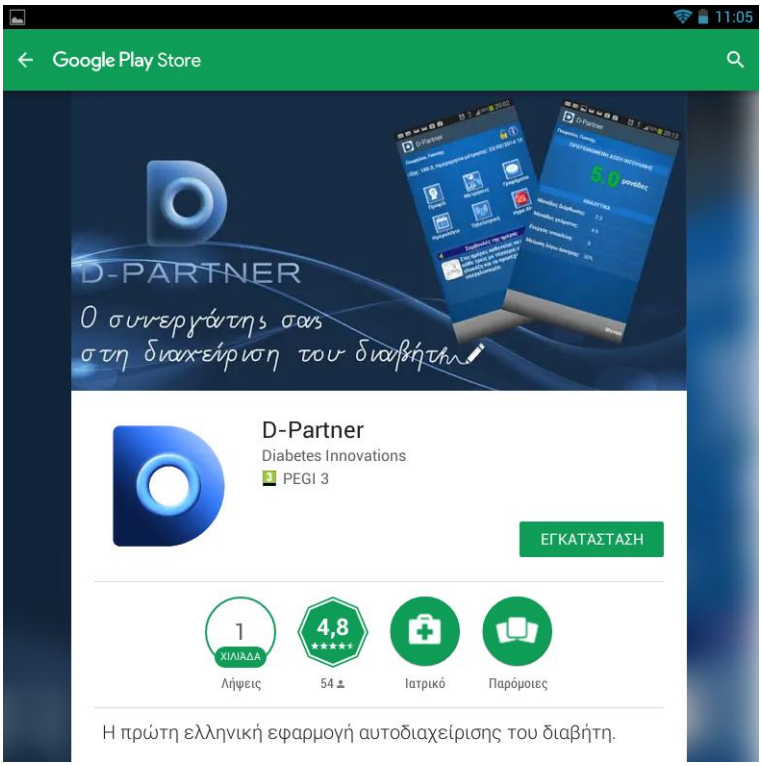
10 . Αρχή της Αναλογικότητας: Κατά την λειτουργία της εφαρμογής, δεν ζητούνται από τον χρήστη πληροφορίες πέραν από αυτές που είναι απαραίτητες. Όμως, οι Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση των Εφαρμογών, όπως η ταυτότητα, οι επαφές, η τοποθεσία, οι Φωτογραφίες/Μέσα/Αρχεία, οι πληροφορίες σύνδεσης Wi-Fi και οι πληροφορίες σύνδεσης Bluetooth, είναι πάρα πολλές και δεν έχουν όλες σχέση με την λειτουργία της εφαρμογής.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Χρησιμοποιείται SSL encryption για την διακίνηση των δεδομένων. Στους όρους Χρήσης αναφέρεται ότι κατά την επεξεργασία των δεδομένων, αφαιρούνται όλες οι προσωπικές πληροφορίες που θα μπορούσαν να ταυτοποιήσουν έναν χρήστη (Ανωνυμοποίηση Δεδομένων).

12. Γονική Συναίνεση: Η Γονική Συναίνεση είναι υποχρεωτική. Επιπλέον, οι Γονείς/Νόμιμοι Κηδεμόνες έχουν το δικαίωμα πρόσβασης στα δεδομένα των -υπό την κηδεμονία τους- ανηλίκων στην εν λόγω εφαρμογή. Δεν διευκρινίζεται όμως πώς θα διαπιστώνεται (με ποια τεχνικά μέσα) η ηλικία του χρήστη και πώς θα παρέχεται η γονική συναίνεση.

Παρατήρηση: Για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα των Χρηστών, η εταιρεία Dottli Ltd έχει προβεί στην σύναψη Συμφωνιών Εμπιστευτικότητας (Confidentiality Agreement) με τους συνεργάτες της, καθώς και με τις συνεργαζόμενες επιχειρήσεις.

5.8 D-partner Application



Εικόνα 5.8: D-partner Application [18]

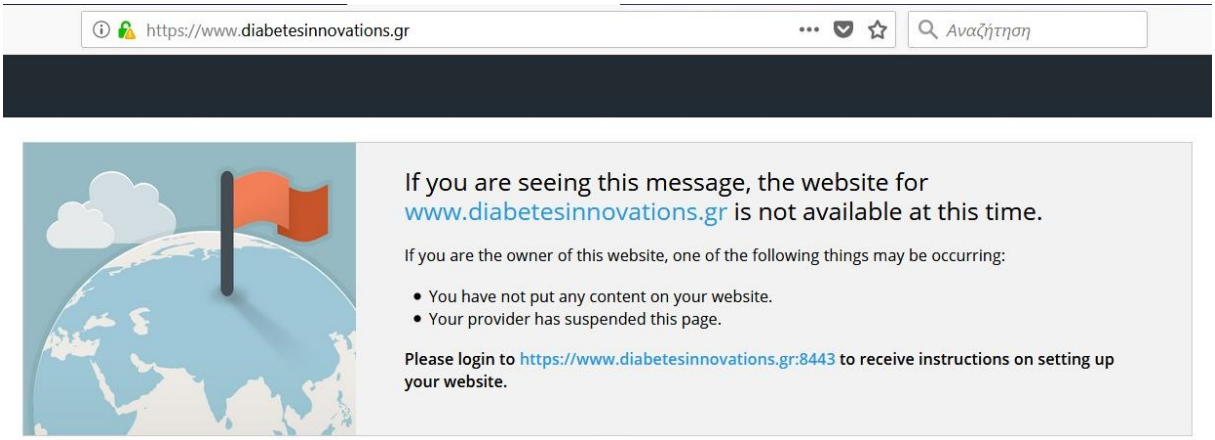
1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Ιστορικό συσκευής και εφαρμογών, Τοποθεσία, SMS, Φωτογραφίες/Μέσα/Αρχεία, Αναγνωριστικό συσκευής/στοιχεία κλήσεων.

Παρατήρηση για τα Κριτήρια 2-12: Δεν ήταν δυνατή η πρόσβαση στους Όρους και Προϋποθέσεις και στην Πολιτική Απορρήτου, παρά μόνο σε κάποιους γενικούς Όρους Χρήσης, οι οποίοι δεν απαντούν ικανοποιητικά στα σχετικά ερωτήματα για: Το Δικαίωμα της Ενημέρωσης, το Δικαίωμα της Πρόσβασης, το Δικαίωμα της Διόρθωσης, το Δικαίωμα της Αντίρρησης – Εναντίωσης, το Δικαίωμα Περιορισμού της Επεξεργασίας, το Δικαίωμα στη Λήθη/της Διαγραφής, το Δικαίωμα στην Φορητότητα των Δεδομένων, το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων, την Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του, την Αρχή της Αναλογικότητας, την Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση) και την Γονική Συναίνεση.

Παρ' όλα αυτά, για να αποκτήσει ο χρήστης πρόσβαση στην εφαρμογή, είναι υποχρεωμένος να «κλικάρει» το check-box: «Δέχομαι» που εμφανιζόταν στο τέλος των Όρων Χρήσης. Με την αποδοχή των όρων αυτών «*ο χρήστης δηλώνει ρητά και ανεπιφύλακτα ότι έχει την νόμιμη ηλικία*

σύμφωνα με το νόμο, που του επιτρέπει τη νομική του δέσμευση από τους παρόντες όρους και ότι έχει διαβάσει και κατανοήσει πλήρως το σύνολο των όρων της παρούσας με τους οποίους συναινεί ανεπιφύλακτα».

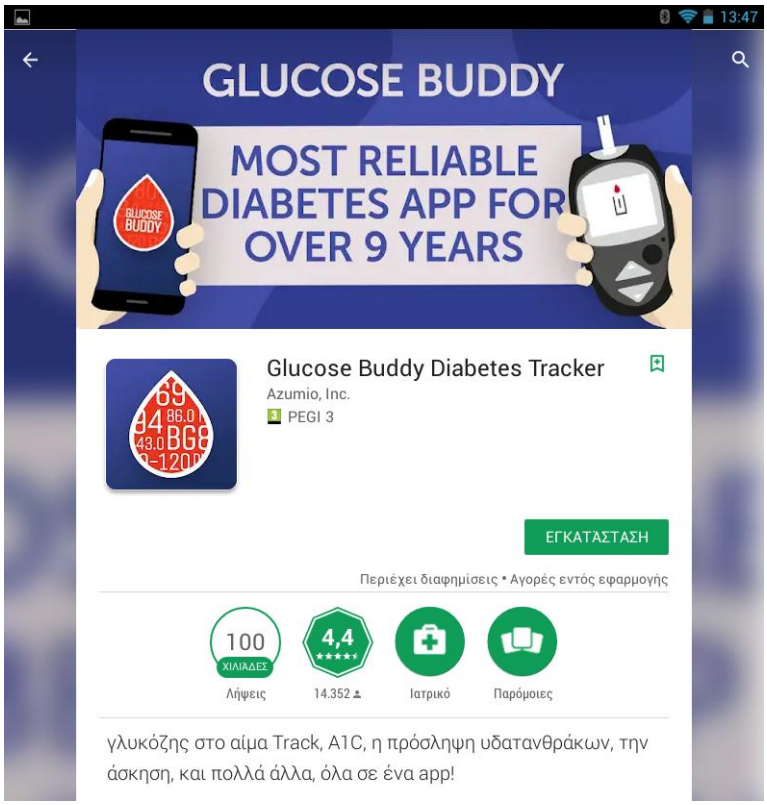
Επειδή είναι η μόνη ελληνική εφαρμογή που εντοπίσαμε, προσπαθήσαμε να την αναλύσουμε περαιτέρω. Διαπιστώσαμε ότι οι σύνδεσμοι για τους Όρους και Προϋποθέσεις και την Πολιτική Απορρήτου, εμφάνιζαν το σφάλμα: "*Server Error 404 Page Not Found. This page either doesn't exist, or it moved somewhere else*". Στην προσπάθειά μας να δούμε την επίσημη ιστοσελίδα της εταιρείας, λάβαμε την ειδοποίηση ότι η ιστοσελίδα δεν είναι διαθέσιμη:



Εικόνα 5.9: Μη διαθέσιμη ιστοσελίδα: www.diabetesinnovations.gr

Από όλες τις παραπάνω πληροφορίες καταλήξαμε στο συμπέρασμα ότι ναι μεν η εφαρμογή είναι διαθέσιμη στο Google Play Store, δεν υποστηρίζεται όμως από την κατασκευάστρια εταιρεία, με ό,τι αυτό συνεπάγεται για την ομαλή λειτουργία της.

5.9 Glucose Buddy Diabetes Tracker Application



Εικόνα 5.10: Glucose Buddy Diabetes Tracker Application [22]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Ταυτότητα, Τοποθεσία, Φωτογραφίες/Μέσα/Αρχεία, Κάμερα

2. Το Δικαίωμα της Ενημέρωσης: Οι Όροι Υπηρεσίας (Terms of Service) και η Πολιτική Απορρήτου (Privacy Policy) είναι πλήρως αναλυτικοί και επεξηγηματικοί. Γίνεται ακόμη και επεξήγηση των σχετικών όρων με παραδείγματα.

3. Το Δικαίωμα της Πρόσβασης: Δεν αναφέρεται κάτι σχετικό, ούτε στην Πολιτική Απορρήτου (Privacy Policy), ούτε στους Όρους της Υπηρεσίας (Terms of Service).

4. Το Δικαίωμα της Διόρθωσης: Στους όρους της υπηρεσίας (Terms of Service) αναφέρει ότι ο χρήστης είναι ο μόνος υπεύθυνος για την ορθότητα και ακρίβεια των δεδομένων του. Εάν αντιληφθεί ότι υπάρχει κάποιο λάθος στα δεδομένα του είναι και ο μόνος που μπορεί να το διορθώσει.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν αναφέρεται κάτι σχετικό, ούτε στην Πολιτική Απορρήτου (Privacy Policy), ούτε στους Όρους της Υπηρεσίας (Terms of Service).

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο χρήστης μπορεί να ζητήσει την διαγραφή των δεδομένων μέσω email. Η διαγραφή όμως αφορά την ενεργή βάση δεδομένων και όχι το αρχείο (archive) της εταιρείας και μόνο μετά το πέρας τυχόν εκκρεμοτήτων, π.χ. μια έρευνα της εταιρείας στην οποία συμμετέχει ο χρήστης.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Στους Όρους της Υπηρεσίας (Terms of Service) αναφέρει ότι ο χρήστης μπορεί να διαγράψει τον λογαριασμό του στην εφαρμογή ανά πάσα στιγμή, δεν αναφέρει όμως αν μπορεί να μεταφέρει τα δεδομένα του σε άλλη εφαρμογή. Υπάρχει μόνο η δυνατότητα εξαγωγής (export) αναφορών σε μορφή pdf. Ως γνωστόν, τα αρχεία της μορφής αυτής προορίζονται μόνο για ανάγνωση, επομένως δεν μπορούν να εισαχθούν ως έχουν σε άλλη εφαρμογή.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Η εφαρμογή δίνει την δυνατότητα στους χρήστες να απενεργοποιήσουν τα cookies. Στην περίπτωση αυτή όμως δεν υπάρχει εγγύηση ότι η εφαρμογή θα λειτουργεί ικανοποιητικά.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Οι Όροι Υπηρεσίας (Terms of Service) και η Πολιτική Απορρήτου (Privacy Policy) είναι πλήρως αναλυτικοί και επεξηγηματικοί. Γίνεται ακόμη και επεξήγηση των σχετικών όρων με παραδείγματα. Επιπλέον, πριν την επιλογή "Sign up" γίνεται σαφή αναφορά ότι επιλέγοντάς τη ο χρήστης συμφωνεί στους Όρους Υπηρεσίας (Terms of Service) και την Πολιτική Απορρήτου (Privacy Policy).

10. Αρχή της Αναλογικότητας: Τα δεδομένα που ζητά η εφαρμογή από τον χρήστη είναι σχετικά με την λειτουργία της π.χ: Φύλο, ηλικία, τιμές γλυκόζης, κτλ. Ωστόσο, στις Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση των Εφαρμογών ζητά –μεταξύ άλλων – την ταυτότητα, την τοποθεσία, τις φωτογραφίες και την κάμερα, δεδομένα που δεν μπορούν να θεωρηθούν απαραίτητα για την εκπλήρωση των σκοπών της εφαρμογής.

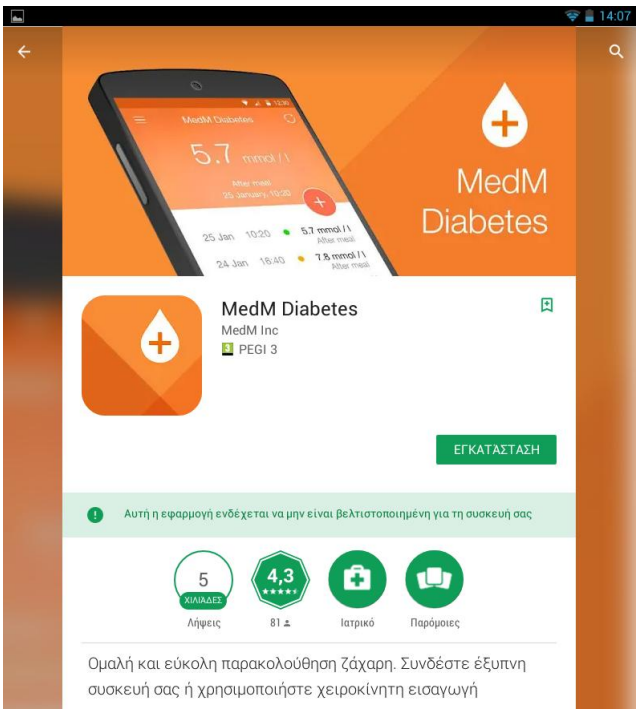
11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Στην Πολιτική Απορρήτου (Privacy Policy) αναφέρεται ότι η εταιρεία χρησιμοποιεί διάφορες

τεχνολογίες ασφάλειας για την προστασία των δεδομένων, χωρίς να υπεισέρχεται σε τεχνικές λεπτομέρειες.

12. Γονική Συναίνεση: Στην Πολιτική Απορρήτου (Privacy Policy) αναφέρεται ρητά ότι η εφαρμογή δεν απευθύνεται σε παιδιά κάτω των 13 ετών. Επιπλέον προτρέπει γονείς και κηδεμόνες που θα αντιληφθούν ότι τα παιδιά τους έχουν στείλει πληροφορίες χωρίς την συγκατάθεσή τους, να το γνωστοποιήσουν στην εταιρεία, για να διαγράψει τις πληροφορίες αυτές. Επίσης, στις ρυθμίσεις της εφαρμογής ζητείται η ηλικία του χρήστη. Βέβαια κι εδώ δεν υπάρχει κάποιο τεχνικό μέσο που να μπορεί να επιβεβαιώσει ότι ο χρήστης εισάγει τα πραγματικά του στοιχεία.

Παρατηρήσεις: Γνωστοποιείται στους χρήστες εκτός Η.Π.Α. ότι η επεξεργασία των δεδομένων τους μπορεί να γίνει στην χώρα που συλλέχθηκαν ή σε άλλη χώρα συμπεριλαμβανομένων των Η.Π.Α. Στο κείμενο αναφέρεται επί λέξει: "*Your personal data may be processed in the country in which it was collected and in other countries, including the United States, where laws regarding processing of Personal Data may be less stringent than the laws in your country*".

5.10 MedM Diabetes Application



Εικόνα 5.11: MedM Diabetes Application [28]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Τοποθεσία, Φωτογραφίες/Μέσα/Αρχεία, Κάμερα, Πληροφορίες σύνδεσης Bluetooth.

2. Το Δικαίωμα της Ενημέρωσης: Ο χρήστης έχει στην διάθεσή του μία αναλυτική Συμφωνία Υπηρεσίας (Service Agreement), η οποία περιέχει τους όρους χρήσης, καθώς και γενικούς νομικούς όρους.

3. Το Δικαίωμα της Πρόσβασης: Δεν αναφέρεται κάτι σχετικό στην Συμφωνία Υπηρεσίας (Service Agreement), αλλά ούτε και στις ρυθμίσεις της εφαρμογής εντοπίστηκε κάποιο σημείο όπου να περιγράφεται μία ανάλογη διαδικασία, που να υπάρχει στον χρήστη την υπηρεσία αυτή.

4. Το Δικαίωμα της Διόρθωσης: Δεν αναφέρεται κάτι σχετικό στην Συμφωνία Υπηρεσίας (Service Agreement), αλλά ούτε και στις ρυθμίσεις της εφαρμογής εντοπίστηκε κάποιο σημείο όπου να περιγράφεται μία ανάλογη διαδικασία, που να υπάρχει στον χρήστη την υπηρεσία αυτή.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν αναφέρεται κάτι σχετικό στην Συμφωνία Υπηρεσίας (Service Agreement), αλλά ούτε και στις ρυθμίσεις της εφαρμογής εντοπίστηκε κάποιο σημείο όπου να περιγράφεται μία ανάλογη διαδικασία, που να υπάρχει στον χρήστη την υπηρεσία αυτή.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Στην Συμφωνία Υπηρεσίας (Service Agreement) αναφέρεται ότι εάν ο χρήστης απωλέσει τα στοιχεία πρόσβασης στην εφαρμογή, τότε χάνει και όλα τα αποθηκευμένα δεδομένα του σε αυτή. Επίσης, εάν ο χρήστης ακυρώσει την εγγραφή του στην υπηρεσία, τότε τα δεδομένα του μπορεί να διαγραφούν από τους servers της. Η λέξη «μπορεί» (“may” στο πρωτότυπο κείμενο) δηλώνει πιθανότητα και όχι βεβαιότητα.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Στην Συμφωνία Υπηρεσίας (Service Agreement) αναφέρεται ότι εάν ο χρήστης απωλέσει τα στοιχεία πρόσβασης στην εφαρμογή, τότε χάνει και όλα τα αποθηκευμένα δεδομένα του σε αυτή.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Δεν αναφέρεται κάτι σχετικό στην Συμφωνία Υπηρεσίας (Service Agreement), αλλά ούτε και στις

ρυθμίσεις της εφαρμογής εντοπίστηκε κάποιο σημείο όπου να περιγράφεται μία ανάλογη διαδικασία, που να υπάρχει στον χρήστη την υπηρεσία αυτή.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Για την είσοδο του χρήστη στην εφαρμογή του δίνονται οι επιλογές: α)Login, β)register και γ)continue without registration. Οι δύο πρώτες επιλογές (login – register) δίνουν την επιπλέον δυνατότητα στον χρήστη να κάνει sync και backup τα δεδομένα του, ώστε να μπορεί να την χρησιμοποιεί από οποιαδήποτε Android συσκευή, ενώ η τρίτη επιλογή (continue without registration) του επιτρέπει απλά να χρησιμοποιεί την εφαρμογή τοπικά σε μία συγκεκριμένη Android συσκευή. Σε καμία όμως από τις περιπτώσεις αυτές δεν του ζητείται μία επικύρωση του τύπου: «με την εγκατάσταση συναινώ στην περιγραφείσα επεξεργασία δεδομένων».

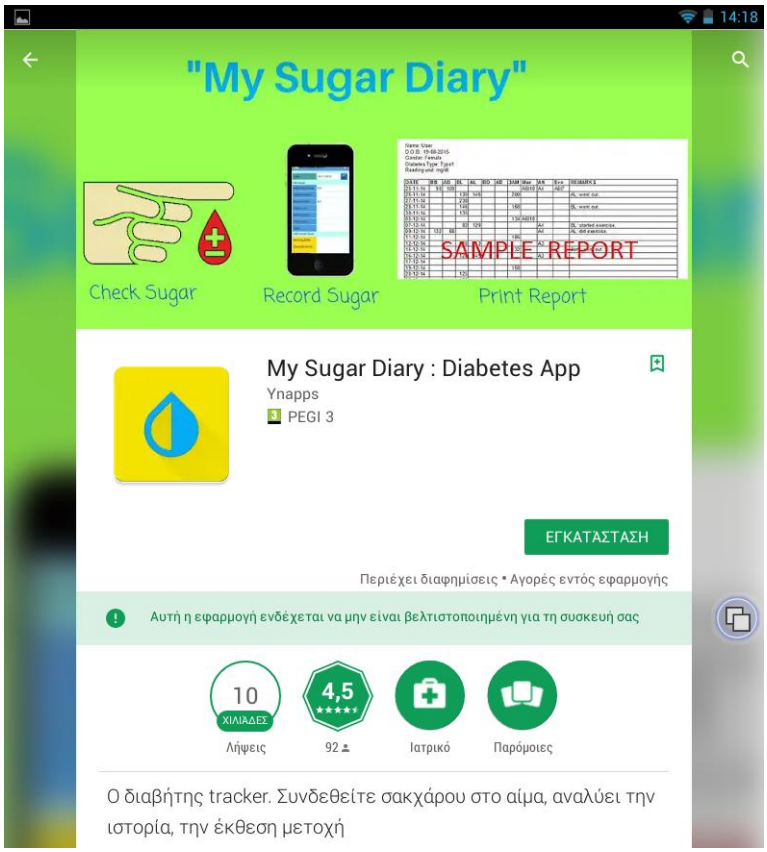
10. Αρχή της Αναλογικότητας: Τα δεδομένα που ζητά η εφαρμογή από τον χρήστη είναι σχετικά με την λειτουργία της π.χ: Φύλο, ηλικία, τιμές γλυκόζης, κτλ, αλλά στις Προαπαιτούμενες Πληροφορίες Χρήστη ζητά –μεταξύ άλλων – την τοποθεσία, τις φωτογραφίες, την κάμερα, καθώς και τις πληροφορίες σύνδεσης Bluetooth, δεδομένα που δεν μπορούν να θεωρηθούν απαραίτητα για την καλή λειτουργία της εφαρμογής.

11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Η σύνδεση της εφαρμογής με τον server της εταιρείας για πρόσβαση στους όρους της Συμφωνία Υπηρεσίας (Service Agreement) είναι κρυπτογραφημένη, μιας και η ιστοσελίδα είναι: https://health.medm.com/ .

12. Γονική Συναίνεση: Η εφαρμογή ζητά την ημερομηνία γέννησης του χρήστη. Βέβαια ο χρήστης μπορεί να εισάγει ό,τι στοιχεία θέλει, αρκεί να έχουν έγκυρη μορφή. Δεν καταφέραμε όμως να εντοπίσουμε κάποια αναφορά ότι – παραδείγματος χάρη - απευθύνεται μόνο σε ενήλικες ή ότι σε περίπτωση ανήλικου χρήστη απαιτείται η γονική συναίνεση.

Παρατήρηση: Η εν λόγω εφαρμογή δεν αξιώνει δικαίωμα ιδιοκτησίας στα δεδομένα που εισάγει ο χρήστης, ούτε ελέγχει την ορθότητά τους. Αναφέρει επί λέξει: "*Your content remains your content*" («*Το περιεχόμενό σας παραμένει δικό σας*»). Παρ' όλα αυτά, στην Συμφωνία Υπηρεσίας (Service Agreement) αναφέρει ότι η εταιρεία έχει το δικαίωμα να επεξεργάζεται όλα τα δεδομένα υγείας που παρέχει ο χρήστης.

5.11 My Sugar Diary Diabetes Application



Εικόνα 5.12: My Sugar Diary Diabetes Application [29]

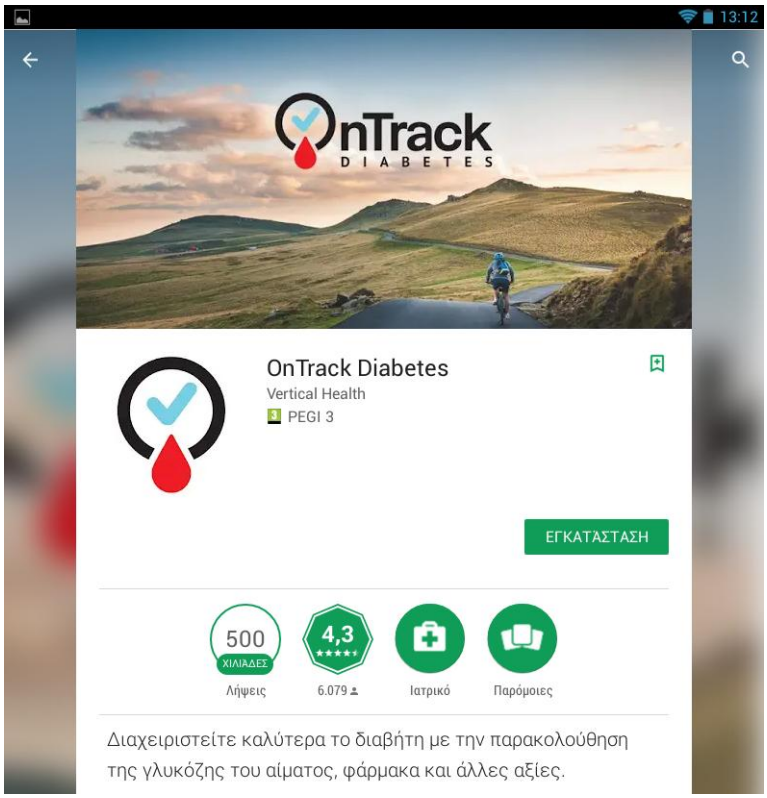
1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Αγορές εντός εφαρμογής, Φωτογραφίες/Μέσα/Αρχεία.

Παρατήρηση για τα Κριτήρια 2-12: Δεν υπάρχουν Όροι Χρήσης ή Πολιτική Ασφάλειας στις επιλογές της εφαρμογής, απ' όπου να είναι δυνατή η εξαγωγή σχετικής πληροφορίας για: Το Δικαίωμα της Ενημέρωσης, το Δικαίωμα της Πρόσβασης, το Δικαίωμα της Διόρθωσης, το Δικαίωμα της Αντίρρησης – Εναντίωσης, το Δικαίωμα Περιορισμού της Επεξεργασίας, το Δικαίωμα στη Λήθη/της Διαγραφής, το Δικαίωμα στην Φορητότητα των Δεδομένων, το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων, την Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του, την Αρχή της Αναλογικότητας, την Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση) και την Γονική Συναίνεση.

Το μόνο στοιχείο που καταφέραμε να εντοπίσουμε είναι ότι δίνεται στον χρήστη η επιλογή αποθήκευσης των δεδομένων του στο Google Drive, ώστε να μπορεί να τα επαναφέρει, σε περίπτωση επανεγκατάστασης της εφαρμογής. Επίσης μπορεί να στείλει μία αναφορά (report)

με κάποια από τα δεδομένα που έχει εισάγει στην εφαρμογή με email ή, αν χρειαστεί, μπορεί να επικοινωνήσει με την εταιρεία μέσω email.

5.12 On Track Diabetes Application



Εικόνα 5.13: On Track Diabetes Application [33]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Φωτογραφίες/Μέσα/Αρχεία.

2. Το Δικαίωμα της Ενημέρωσης: Ένα πολυσέλιδο έγγραφο με τίτλο: Όροι Χρήσης για εφαρμογές κινητών (Mobile Applications Terms of Use) είναι στην διάθεση του χρήστη.

3. Το Δικαίωμα της Πρόσβασης: Δεν υπάρχει σχετική αναφορά στους Όρους Χρήσης (Terms of Use), αλλά ούτε και σε κάποιο άλλο σημείο της εφαρμογής.

4. Το Δικαίωμα της Διόρθωσης: Δεν υπάρχει σχετική αναφορά στους Όρους Χρήσης (Terms of Use), αλλά ούτε και σε κάποιο άλλο σημείο της εφαρμογής.

5. Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν υπάρχει σχετική αναφορά στους Όρους Χρήσης (Terms of Use), αλλά ούτε και σε κάποιο άλλο σημείο της εφαρμογής.

6. Το Δικαίωμα στη Λήθη/της Διαγραφής: Ο χρήστης έχει την δυνατότητα να διαγράψει τον λογαριασμό του και να απεγκαταστήσει την εφαρμογή από την συσκευή του, αλλά τα δεδομένα του παραμένουν στους servers τη εταιρείας.

7. Το Δικαίωμα στη Φορητότητα των Δεδομένων: Ο χρήστης έχει την δυνατότητα να κρατήσει backup των δεδομένων του στην SD card της συσκευής του, ή να τα κάνει export σε μορφή CSV (comma-separated values), αλλά δεν μπορεί να αξιοποιήσει την πληροφορία αυτή πέραν της συγκεκριμένης εφαρμογής. Η μορφή αρχείου CSV μπορεί να ανοιχθεί και να επεξεργαστεί στο Microsoft Excel, αλλά αυτό δεν συνεπάγεται ότι κάποια άλλη m-Health εφαρμογή για τον Σακχαρώδη Διαβήτη θα αναγνωρίσει και θα αξιοποιήσει τα δεδομένα αυτά.

8. Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Δεν υπάρχει σχετική αναφορά στους Όρους Χρήσης (Terms of Use), αλλά ούτε και σε κάποιο άλλο σημείο της εφαρμογής.

9. Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Υπάρχει check box στο σημείο: "Legal Stuff", το οποίο ο χρήστης πρέπει να επιλέξει για να συνεχίσει στην εφαρμογή. Με την επιλογή του κουτιού αυτού ο χρήστης δηλώνει ότι συμφωνεί με όσα η Άδεια Τελικού Χρήστη ορίζει ("By checking this, I agree to the: End User License Agreement").

10. Αρχή της Αναλογικότητας: Τα δεδομένα που ζητά η εφαρμογή από τον χρήστη είναι σχετικά με την λειτουργία της π.χ: Φύλο, ηλικία, τιμές γλυκόζης, κτλ.

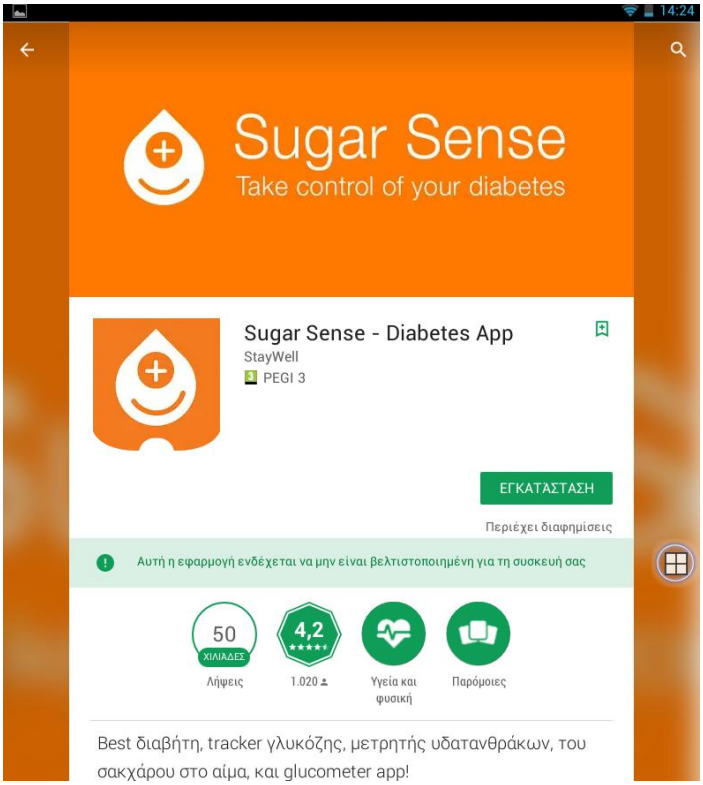
11. Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Δεν κατέστη δυνατή η εξακρίβωση ύπαρξης κάποιας συγκεκριμένης μορφής κρυπτογράφησης. Πάντως, ο σύνδεσμος που παραπέμπει στους Όρους Χρήσης (Terms of Use) της εφαρμογής δεν παραπέμπει σε ασφαλή ιστοσελίδα (http://www.prognos.ai/mobile-applications-terms-service).

12. Γονική Συναίνεση: Δεν υπάρχει σχετική αναφορά στους Όρους Χρήσης (Terms of Use) της εφαρμογής. Επίσης, δεν εντοπίσαμε κάποια αναφορά ότι αυτή η εφαρμογή απευθύνεται

σε ηλικίες άνω των 16 ή άνω των 18 και δεν υπάρχει καν ένα check-box στο οποίο ο χρήστης να έχει την δυνατότητα να δηλώσει την ηλικία του ή το αν είναι ενήλικος.

Παρατήρηση: Η εφαρμογή υπόκειται στους νόμους της πολιτείας της Νέας Υόρκης των Η.Π.Α.

5.13 Sugar Sense Diabetes Plus Application



Εικόνα 5.14: Sugar Sense Diabetes Plus Application [39]

1. Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση της Εφαρμογής: Ιστορικό συσκευής και εφαρμογών, Ταυτότητα, Φωτογραφίες/Μέσα/Αρχεία, Κάμερα, Αναγνωριστικό συσκευής/στοιχεία κλήσεων

Παρατήρηση για τα Κριτήρια 2-12: Υπήρχαν σύνδεσμοι (links) για τους Όρους και Προϋποθέσεις (Terms & Conditions), καθώς και για Πολιτική Ασφάλειας (Privacy Policy), αλλά στην προσπάθεια προσπέλασής τους, εμφανιζόταν το μήνυμα: "Webpage not available". Έτσι δεν ήταν εύκολο να εξαχθούν συμπεράσματα για: Το Δικαίωμα της Ενημέρωσης, το Δικαίωμα της Πρόσβασης, το Δικαίωμα της Διόρθωσης, το Δικαίωμα της Αντίρρησης – Εναντίωσης, το Δικαίωμα Περιορισμού της Επεξεργασίας, το Δικαίωμα στη Λήθη/της Διαγραφής, το Δικαίωμα στην Φορητότητα των Δεδομένων, το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη

Αποφάσεων, την Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του, την Αρχή της Αναλογικότητας, την Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση) και την Γονική Συναίνεση.

Τα μόνα ζητήματα που στοιχειοθετήθηκαν είναι ότι: α) οι προαπαιτούμενες πληροφορίες από τον χρήστη για την εγκατάσταση της Εφαρμογής είναι πάρα πολλές και δεν έχουν εμφανή σχέση με το αντικείμενό της, όπως το ιστορικό της συσκευής και των εφαρμογών, η ταυτότητα, οι φωτογραφίες, η κάμερα και το αναγνωριστικό της συσκευής και τα στοιχεία κλήσεων. β) Η εφαρμογή ζητά την ημερομηνία γέννησης του χρήστη. Βέβαια ο χρήστης μπορεί να εισάγει ό,τι στοιχεία θέλει, αρκεί να έχουν έγκυρη μορφή. Από την στιγμή όμως, που δεν λειτουργούσαν οι σύνδεσμοι για τους Όρους και Προϋποθέσεις (Terms & Conditions), καθώς και για Πολιτική Ασφάλειας (Privacy Policy), δεν ήταν εφικτός ο εντοπισμός κάποιας αναφοράς ότι – παραδείγματος χάρη – η εφαρμογή απευθύνεται μόνο σε ενήλικες ή ότι σε περίπτωση ανήλικου χρήστη απαιτείται η γονική συναίνεση.

Κεφάλαιο 6
Αποτελέσματα - Συμπεράσματα

Στο προηγούμενο κεφάλαιο έγινε μελέτη δώδεκα (12) m-Health εφαρμογών με αντικείμενο την διαχείριση των Δεδομένων Προσωπικού Χαρακτήρα χρηστών με Σακχαρώδη Διαβήτη. Στο κεφάλαιο πραγματοποιείται μία ανάλυση των αποτελεσμάτων αυτών, προκειμένου να φθάσουμε σε ασφαλή συμπεράσματα για τον βαθμό διασφάλισης των Δεδομένων Προσωπικού Χαρακτήρα στις εφαρμογές αυτές.

Πρώτ' απ' όλα, συντάξαμε έναν συγκεντρωτικό πίνακα των εφαρμογών, καθώς και των κριτηρίων, με βάση τα οποία αναλύσαμε τις εφαρμογές αυτές. Για μεγαλύτερη ευκολία στην διαχείριση των δεδομένων, καταλήξαμε να χρησιμοποιήσουμε τους παρακάτω συμβολισμούς:

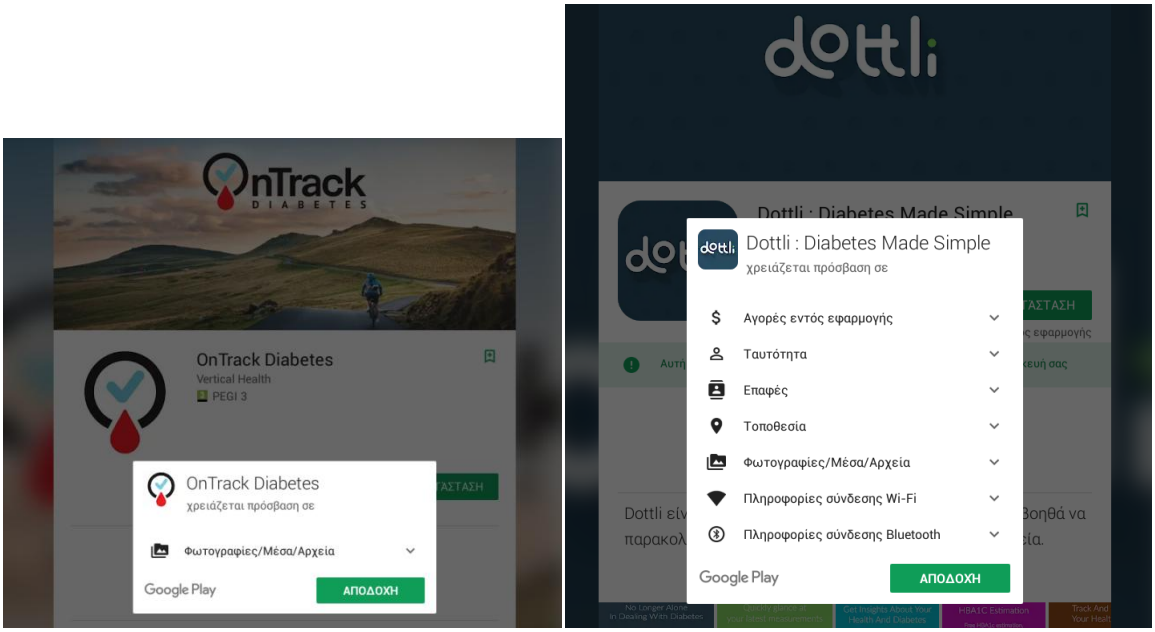
A1–A12 (όπου A=Application): Ο αύξων αριθμός των εφαρμογών, όπως αυτές παρουσιάστηκαν, δηλαδή με αλφαβητική σειρά.
C1–C12 (όπου C=Criterion): Ο αύξων αριθμός των κριτηρίων, όπως αυτά παρουσιάστηκαν στο προηγούμενο κεφάλαιο.

	A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**	**A9**	**A10**	**A11**	**A12**	
C1	2	2	2	4	1	7	5	5	4	2	1	5	**Σύνολο:**
C2	1	0	0	1	0	1	0	1	1	0	1	0	**6**
C3	1	0	1	0	0	1	0	0	0	0	0	0	**3**
C4	0	0	1	0	0	1	0	1	0	0	0	0	**3**
C5	0	0	0	0	0	0	0	0	0	0	0	0	**0**
C6	1	0	0	0	1	0	0	0	0	0	0	0	**2**
C7	0	0	0	0	0	0	0	0	0	0	0	0	**0**
C8	0	0	0	0	0	1	0	1	0	0	0	0	**2**
C9	0	0	0	1	0	1	0	1	0	0	1	0	**4**
C10	1	1	1	0	1	0	0	0	0	0	1	0	**5**
C11	0	0	1	0	0	1	0	1	1	1	0	0	**5**
C12	0	0	0	1	0	1	0	1	0	0	0	0	**3**
Σύνολο:	**4**	**1**	**4**	**3**	**2**	**7**	**0**	**6**	**2**	**1**	**3**	**0**	

Πίνακας 6.1: Συγκεντρωτικός πίνακας m-Health εφαρμογών

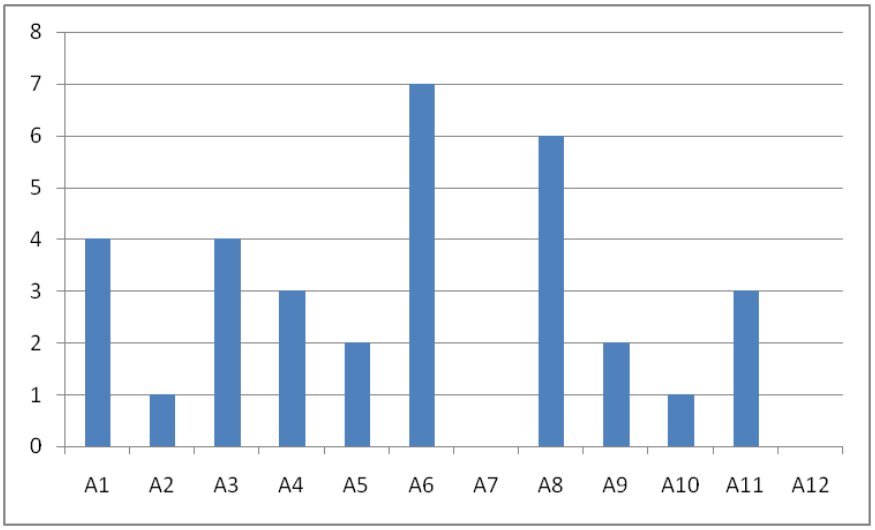
Όπως εύκολα μπορεί να διαπιστώσει κανείς, οι γραμμές του πίνακα αντιστοιχούν στα κριτήρια και οι στήλες στις εφαρμογές. Για κάθε ένα κριτήριο που ικανοποιούσε μία εφαρμογή, αναγράφεται η τιμή «1» στο αντίστοιχο κελί, ενώ αντίθετα, όταν μία εφαρμογή δεν πληρούσε ένα κριτήριο αναγράφεται η τιμή «0». Στην τελευταία γραμμή και αντίστοιχα, στην τελευταία στήλη, μπορεί να δει κανείς το άθροισμα των βαθμών για κάθε κριτήριο ή κάθε εφαρμογή.

Οφείλουμε να σημειώσουμε ότι στις πράξεις αυτές δεν συμμετέχει το πρώτο κριτήριο, καθώς δεν λαμβάνει τις τιμές «1» και «0», μιας και περιέχει (σε απόλυτους αριθμούς) το πλήθος των προαπαιτούμενων Πληροφοριών Χρήστη για την εγκατάσταση της κάθε εφαρμογής. Πιο συγκεκριμένα, βλέπουμε ότι ο αριθμός των προαπαιτούμενων πληροφοριών χρήστη ποικίλει από εφαρμογή σε εφαρμογή και κυμαίνεται από τον αριθμό 1 έως το 7. Για του λόγου το αληθές, παραθέτουμε δύο χαρακτηριστικά screenshots, ένα από μία εφαρμογή με τις λιγότερες απαιτήσεις (1) και ένα από αυτήν με τις περισσότερες (7):



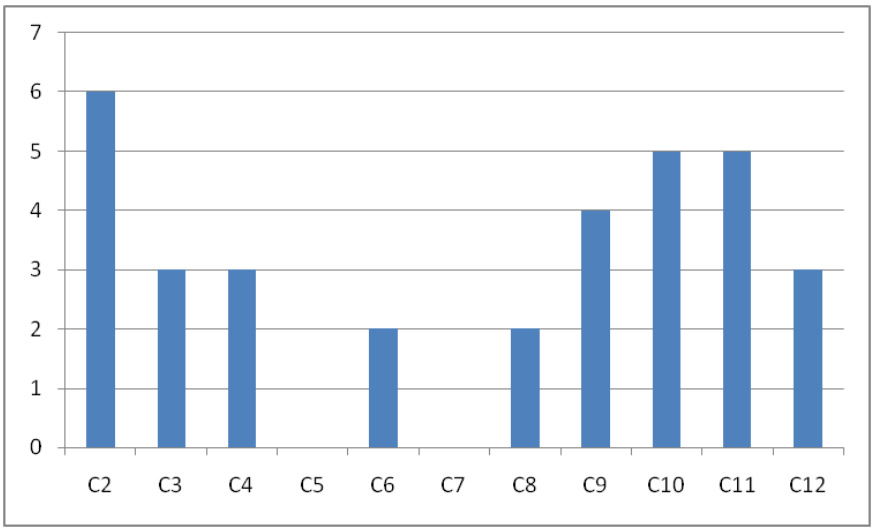
Εικόνες 6.1 και 6.2: Προαπαιτούμενες Πληροφορίες Χρήστη για την εγκατάσταση της κάθε εφαρμογής.

Έχοντας σαν βάση τον πίνακα 6.1, δημιουργήσαμε δύο αντίστοιχα γραφήματα. Στο πρώτο γράφημα εμφανίζεται το πλήθος των κριτηρίων που ικανοποιούνται ανά εφαρμογή, ενώ στο δεύτερο παρουσιάζεται το άθροισμα των εφαρμογών που πληρούν το κάθε κριτήριο. Έτσι έχουμε:



Γράφημα 6.1: Πλήθος κριτηρίων που ικανοποιούνται ανά εφαρμογή

Στο παραπάνω γράφημα φαίνεται ξεκάθαρα ότι από τις 12 συνολικά εφαρμογές m-Health που μελετήσαμε, μόνο δύο (A6 και A8) βρίσκονται σε ένα ικανοποιητικό επίπεδο, όσον αφορά την προστασία των Δεδομένων Προσωπικού Χαρακτήρα των χρηστών. Επίσης, μπορούμε να πούμε ότι τέσσερις ακόμη (A1, A3, A4 και A11) ενημερώνουν τον χρήστη για τα δικαιώματα και τις υποχρεώσεις που απορρέουν από την εγκατάσταση και χρήση της εφαρμογής, έστω σε μία πολύ γενική βάση. Επιπλέον, σε τέσσερις εφαρμογές (A2, A5, A9 και A10) καταφέραμε να εξάγουμε κάποια συμπεράσματα εμμέσως (κάνοντας χρήση της εφαρμογής), χωρίς όμως να μπορούμε να στοιχειοθετήσουμε ότι υπάρχει επαρκής ενημέρωση του χρήστη για τα δικαιώματά του και την προστασία τους. Τέλος, υπήρξαν και δύο εφαρμογές (A7 και A12), για τις οποίες δεν υπήρξε κανένα απολύτως αποτέλεσμα.



Γράφημα 6.2: Άθροισμα εφαρμογών που πληρούν το κάθε κριτήριο

Από το πιο πάνω γράφημα μπορούμε – για το κάθε κριτήριο ξεχωριστά - να αναφέρουμε τα εξής:

C1-Προαπαιτούμενες Πληροφορίες Χρήστη για την Εγκατάσταση των Εφαρμογών: Το κριτήριο αυτό δεν εμφανίζεται στο γράφημα 6.2, αλλά μόνο στον πίνακα 6.1 κι αυτό γιατί, στην ουσία, αποτελεί παράγοντα αξιολόγησης για το αν πληρούται η Αρχή της Αναλογικότητας στις εφαρμογές m-Health. Πιο συγκεκριμένα, βλέπουμε ότι ο αριθμός των προαπαιτούμενων πληροφοριών χρήστη ποικίλει από εφαρμογή σε εφαρμογή και κυμαίνεται από τον αριθμό 1 έως το 7. Αυτό που μένει ως συμπέρασμα είναι ότι όσο μεγαλύτερος είναι ο αριθμός αυτός, τόσο μικρότερη είναι η κλίμακα ισχύς της Αρχής της Αναλογικότητας(C11).

C2-Το Δικαίωμα της Ενημέρωσης: Ικανοποιείται σε έξι από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε, δηλαδή τις μισές. Στις εφαρμογές αυτές, όντως υπάρχει *ενημέρωση για κάθε πληροφορία ή/και ανακοίνωση σχετικά με την επεξεργασία, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση*, όπως ορίζει η κείμενη νομοθεσία.

C3-Το Δικαίωμα της Πρόσβασης: Ικανοποιείται σε τρεις από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε, δηλαδή σε ποσοστό 25%. Φαίνεται ξεκάθαρα ότι οι σχεδιαστές - προγραμματιστές των m-Health εφαρμογών δεν λαμβάνουν σοβαρά υπόψη τους το δικαίωμα αυτό των χρηστών.

C4-Το Δικαίωμα της Διόρθωσης: Ικανοποιείται σε τρεις από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε, δηλαδή σε ποσοστό 25%. Με λίγα λόγια ακολουθεί κι αυτό την μοίρα του Δικαιώματος της Πρόσβασης.

C5-Το Δικαίωμα Περιορισμού της Επεξεργασίας: Δεν αναφέρεται σε καμία από τις εφαρμογές που μελετήσαμε. Δυστυχώς πολλές εφαρμογές δεν ενημερώνουν καν τους χρήστες για το εάν (και ποια) δεδομένα τους επεξεργάζονται κεντρικά οι εταιρείες ή συνεργάτες αυτών, πόσο μάλλον να υπάρχει ενημέρωση και για το Δικαίωμα Περιορισμού της Επεξεργασίας.

C6-Το Δικαίωμα στη Λήθη/της Διαγραφής: Ικανοποιείται σε δύο από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Με τα δεδομένα αυτά, δεν μπορούμε σε καμία περίπτωση να πούμε ότι είναι κοινή λογική στους σχεδιαστές – προγραμματιστές. Ο χρήστης, στις περισσότερες εφαρμογές, έχει την δυνατότητα να διαγράψει τοπικά τα δεδομένα που έχει αποθηκευμένα στην συσκευή του, αλλά ενημέρωση για το τι ισχύει για τα δεδομένα που αποθηκεύει σε servers ή cloud δεν έχει.

C7-Το Δικαίωμα στη Φορητότητα των Δεδομένων: Δεν αναφέρεται σε καμία από τις εφαρμογές που μελετήσαμε. Όμως, οφείλουμε να αναφέρουμε ότι σε πολλές εφαρμογές οι χρήστες μπορούν να κάνουν εξαγωγή των δεδομένων που έχουν εισάγει στην συσκευή τους, αλλά τα αρχεία αυτά είναι κυρίως σε μορφή pdf (reports), με κάποιες μόνο εφαρμογές να δίνουν την δυνατότητα εξαγωγής σε μορφή CSV, αλλά και πάλι, τα δεδομένα αυτά δεν μπορούν να εισαχθούν σε άλλη εφαρμογή χωρίς να πρέπει να υποστούν επεξεργασία. Η μόνη περίπτωση φορητότητας που αναφέρθηκε ήταν από μία εφαρμογή μίας συγκεκριμένης εταιρείας, σε συγκεκριμένη εφαρμογή της ίδιας εταιρείας και γι' αυτό δεν ήταν δυνατό να προσμετρηθεί ως πληρούμενο κριτήριο.

C8-Το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων: Ικανοποιείται σε μόλις δύο από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Στις περισσότερες εφαρμογές δε, δεν υπήρχε καν ενημέρωση του χρήστη για το αν χρησιμοποιούνται τα δεδομένα του για αυτοματοποιημένη λήψη αποφάσεων, πόσο μάλλον να του παρασχεθεί και η οποιαδήποτε διαδικασία για την προστασία του Δικαιώματος της Εναντίωσης σε αυτή.

C9-Ρητή και Σαφή Συγκατάθεση Υποκειμένου για Επεξεργασία των Δεδομένων του: Ικανοποιείται σε τέσσερις από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε, δηλαδή στο 1/3 αυτών. Πρόκειται για ένα σχετικά υψηλό ποσοστό, συγκρινόμενο πάντα με τα υπόλοιπα ευρήματα. Στην ουσία, στις τέσσερις αυτές εφαρμογές ο χρήστης καλούνταν να επιβεβαιώσει ότι συμφωνεί με τους Όρους Χρήσης ή/και την Πολιτική Ασφάλειας (π.χ. Terms of Use or/and Security Policy, ανάλογα με την εφαρμογή), επιλέγοντας ένα αντίστοιχο check-box.

C10-Αρχή της Αναλογικότητας: Φαίνεται ότι ικανοποιείται - στο βαθμό που μπορεί να αποτιμηθεί η αναγκαιότητα και προσφορότητα των δεδομένων που ζητούνται - σε πέντε από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Φτάσαμε στον αριθμό αυτό, γιατί παρ' όλο που (στην συντριπτική τους πλειοψηφία) τα δεδομένα που καλούνταν να εισάγει ο χρήστης στις εφαρμογές m-Health ήταν σχετικά με το αντικείμενο και τους σκοπούς τους, σε κάποιες από αυτές, οι προαπαιτούμενες πληροφορίες από την συσκευή του χρήστη (ταυτότητα, τοποθεσία, κάμερα, επαφές, στοιχεία σύνδεσης Wi-Fi ή Bluetooth, κτλ) ήταν τόσες πολλές που δεν συνάδουν με την Αρχή της Αναλογικότητας.

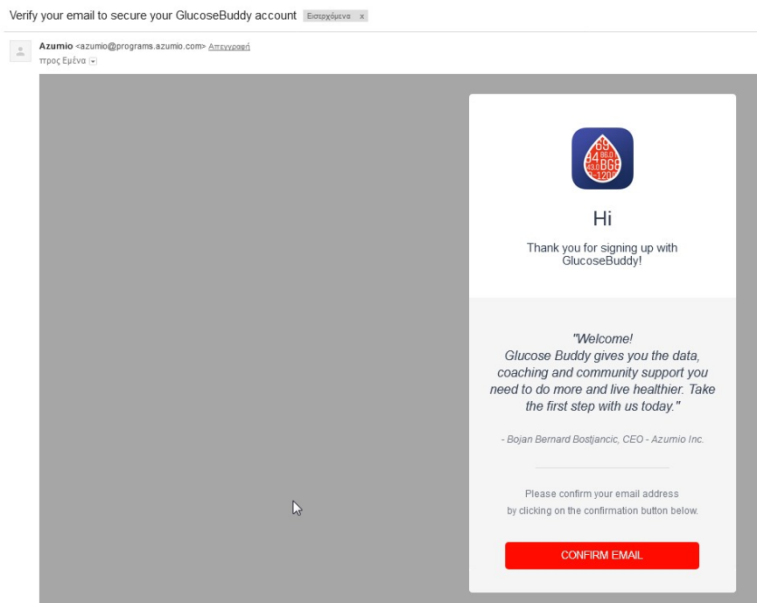
C11-Κρυπτογράφηση των Δεδομένων (Ψευδωνυμοποίηση/Ανωνυμοποίηση): Ικανοποιείται σε πέντε από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Αν και το ποσοστό

αυτό είναι πολύ καλύτερο από αυτά των περισσότερων κριτηρίων, παραμένει χαμηλό για ένα κριτήριο που έχει ίσως την μεγαλύτερη σημασία για την ασφάλεια των δεδομένων του χρήστη.

C12-Γονική Συναίνεση: Ικανοποιείται σε μόλις τρεις από τις δώδεκα συνολικά εφαρμογές που αναλύσαμε, δηλαδή στο 25% του συνόλου. Το ποσοστό αυτό είναι τρομερά χαμηλό για ένα τόσο ευαίσθητο θέμα, όσο η προστασία των παιδιών. Είναι πραγματικά λυπηρό το γεγονός ότι οι περισσότεροι από τους σχεδιαστές – προγραμματιστές των εφαρμογών αυτών, δεν μπήκαν καν στον κόπο να δηλώσουν εάν η εφαρμογή τους απευθύνεται αποκλειστικά σε ενήλικες ή όχι. Κι αν απευθύνεται και σε παιδιά, να απαιτείται, παραδείγματος χάρη, το email ή το τηλέφωνο του γονέα/κηδεμόνα για να λάβει γνώση από την εφαρμογή και να δώσει την συγκατάθεσή του ή όχι.

Γενικά, η εξακρίβωση της ορθότητας των στοιχείων που εισάγει ο χρήστης σε μία m-Health εφαρμογή, είναι ένα πολύ δύσκολο ζήτημα σε τεχνικό, αλλά και νομικό επίπεδο, το οποίο αναλύεται σε κάποια άρθρα και μελέτες, όπως το πρόσφατο (16/04/2018) άρθρο 29 της ομάδας εργασίας της ΕΕ περί οδηγιών συμμόρφωσης με τον ΓΚΠΔ (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

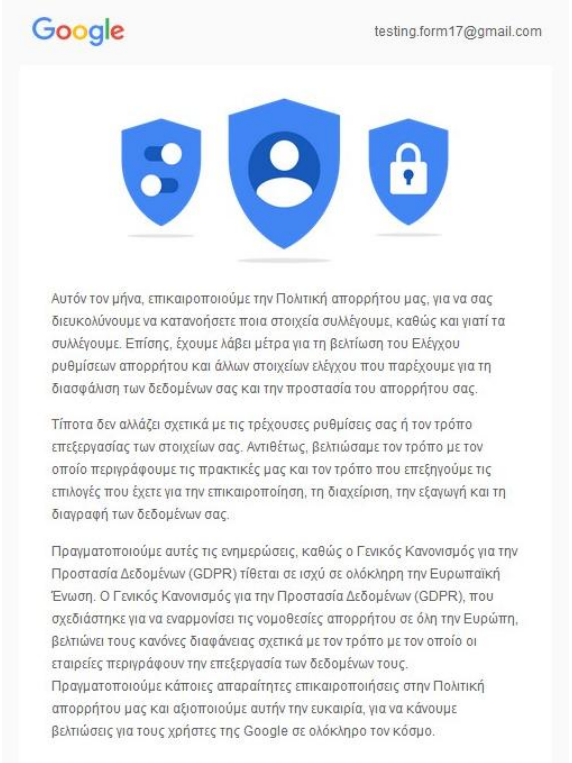
Ένα χαρακτηριστικό παράδειγμα είναι ότι από όλες τις εφαρμογές που μελετήθηκαν στην παρούσα μεταπτυχιακή διατριβή, μόνο μία ζήτησε να επιβεβαιώσουμε τον λογαριασμό μας μέσω του email που δώσαμε:



Εικόνα 6.3: Επιβεβαίωση email χρήστη για τη εφαρμογή GlucoseBuddy

Πιο συγκεκριμένα, τα μόνα –σχετικά με την παρούσα μεταπτυχιακή διατριβή - εισερχόμενα μηνύματα που είχε το email που δημιουργήσαμε στο www.gmail.com ήταν το παραπάνω και ένα ακόμη από την ίδια την Google, με τίτλο: «*Βελτιώσεις στην Πολιτική απορρήτου και στα Στοιχεία ελέγχου διαχείρισης απορρήτου*».

Το συγκεκριμένο email ελήφθη λίγες ημέρες πριν την ολοκλήρωση συγγραφής της συγκεκριμένης μεταπτυχιακής διατριβής και επιλέξαμε να το επισημάνουμε γιατί είναι ένα πολύ καλό παράδειγμα προσαρμογής στην ισχύουσα νομοθεσία.



Εικόνες 6.4 και 6.5: Ενημέρωση των χρηστών για την αναθεωρημένη Πολιτική Απορρήτου της Google

Όπως βλέπουμε στις παραπάνω εικόνες, η Google φαίνεται να έχει να κάνει – βάσει των όσων αναφέρει στην αναθεωρημένη πολιτική της – βήματα προσαρμογής με τις επιταγές των διατάξεων του ΓΚΠΔ. Μία τέτοιου τύπου ενημέρωση, ως πρώτο βήμα, θα πρέπει να γίνει, ή μάλλον να είχε ήδη γίνει και για τις mobile εφαρμογές, τις οποίες, όπως είδαμε και στην

Εισαγωγή αυτής της μεταπτυχιακής διατριβής, τις χρησιμοποιούν δισεκατομμύρια χρήστες ανά την υφήλιο.

Σύμφωνα με τα παραπάνω ευρήματα, απαντώνται τα ερευνητικά ερωτήματα ως ακολούθως:

H1: Είναι η επεξεργασία προσωπικών δεδομένων σύμφωνη με τις βασικές προϋποθέσεις νομιμότητας του ΓΚΠΔ;

Από την ανάλυση των αποτελεσμάτων που πραγματοποιήσαμε στο παρόν κεφάλαιο, διαπιστώθηκαν σοβαρές ελλείψεις όσον αφορά την συμμόρφωση των m-Health εφαρμογών με τις βασικές προϋποθέσεις νομιμότητας του ΓΚΠΔ. Αξιοσημείωτο είναι ότι μόλις οι μισές (6/12) από αυτές ενημέρωναν τους χρήστες για τους Όρους Χρήσης και την Πολιτική Απορρήτου που ακολουθούν και ακόμη λιγότερες (4/12), ζητούσαν ρητή και σαφή συγκατάθεση του χρήστη για επεξεργασία των δεδομένων του.

Επιπλέον, η Αρχή της Αναλογικότητας ικανοποιείται σε πέντε από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Φτάσαμε στον αριθμό αυτό, γιατί παρ' όλο που (στην συντριπτική τους πλειοψηφία) τα δεδομένα που καλούνταν να εισάγει ο χρήστης στις εφαρμογές m-Health ήταν σχετικά με το αντικείμενο και τους σκοπούς τους, σε αρκετές από αυτές, οι προαπαιτούμενες πληροφορίες από την συσκευή του χρήστη (ταυτότητα, τοποθεσία, κάμερα, επαφές, στοιχεία σύνδεσης Wi-Fi ή Bluetooth, κτλ) ήταν τόσες πολλές έθεταν σοβαρά ζητήματα για την προστασία της Ιδιωτικότητας των χρηστών.

Επίσης, μέριμνα για την Γονική Συναίνεση λαμβάνεται σε μόλις τρεις από τις δώδεκα συνολικά εφαρμογές που αναλύσαμε. Το ποσοστό αυτό είναι τρομερά χαμηλό για ένα τόσο ευαίσθητο θέμα, όσο η προστασία των παιδιών. Χαρακτηριστικό παράδειγμα είναι το γεγονός ότι απουσιάζει έστω και μία δήλωση για το εάν η εφαρμογή απευθύνεται αποκλειστικά σε ενήλικες ή όχι. Με βάση όλα τα παραπάνω, δεν μπορεί να υπάρξει θετική απάντηση στο ερώτημα αυτό.

H2: Ικανοποιούνται τα δικαιώματα των χρηστών που προβλέπονται στον ΓΚΠΔ;

Όπως αναφέραμε και στο Κεφάλαιο 5, το Δικαίωμα Περιορισμού της Επεξεργασίας, το Δικαίωμα στη Λήθη/της Διαγραφής, το Δικαίωμα στην Φορητότητα των Δεδομένων και το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων, είναι απαιτήσεις που συναντούμε για πρώτη φορά στον ΓΚΠΔ, του οποίου η τελική ημερομηνία υποχρέωσης συμμόρφωσης με τις

διατάξεις του είναι η 25η Μαΐου 2018, δηλαδή λίγες ημέρες μετά την ολοκλήρωση της μελέτης μας.

Στην κατάταξη των κριτηρίων που πραγματοποιήσαμε στην μελέτη μας, τα κριτήρια αυτά (C5 – C8 στο γράφημα 6.2) έλαβαν τις χαμηλότερες βαθμολογίες. Πιο συγκεκριμένα, καμία εφαρμογή δεν πληρούσε το Δικαίωμα Περιορισμού της Επεξεργασίας και το Δικαίωμα στην Φορητότητα των Δεδομένων, ενώ τα άλλα δύο: Το Δικαίωμα στη Λήθη/της Διαγραφής και το Δικαίωμα Εναντίωσης στην Αυτοματοποιημένη Λήψη Αποφάσεων ικανοποιούνταν μόνο σε δύο εφαρμογές το καθένα. Η απάντηση στο ερώτημα αυτό λοιπόν, δεν μπορεί παρά να είναι αρνητική.

H3: Είναι η επεξεργασία των δεδομένων ασφαλής;

Στοιχεία για ύπαρξη τεχνικών κρυπτογράφησης των δεδομένων των χρηστών κατέστη δυνατόν να εντοπιστούν σε πέντε από τις συνολικά δώδεκα εφαρμογές που αναλύσαμε. Το ποσοστό αυτό είναι πολύ χαμηλό για ένα κριτήριο που έχει ίσως την μεγαλύτερη σημασία για την ασφάλεια των δεδομένων του χρήστη.

Οφείλουμε να συμπληρώσουμε επίσης ότι, παρά το γεγονός ότι η χρήση βιβλιοθηκών τρίτων μερών (third-parties libraries) είναι κοινή πρακτική κατά την ανάπτυξη m-Health εφαρμογών, πολύ λίγες από τις εφαρμογές που μελετήσαμε αναφέρονται σε αυτό και μόνο μία αναφέρει τις βιβλιοθήκες που χρησιμοποιεί και από αυτές, οι μισές δεν εμφανίζονται να χρησιμοποιούν κάποια τεχνική κρυπτογράφησης. Δεν μπορούμε λοιπόν να ισχυριστούμε ότι το συγκεκριμένο ερώτημα απαντάται θετικά.

Κεφάλαιο 7
Επίλογος

Οι εφαρμογές m-Health έχουν αποκτήσει μία απίστευτη δυναμική και την στιγμή αυτή είναι ευρέως διαδεδομένες στους χρήστες «έξυπνων» κινητών τηλεφώνων (smartphones) και tablets. Όμως, παρά την θερμή τους αποδοχή, οι εφαρμογές αυτές έχουν εγείρει σοβαρές ανησυχίες, όσον αφορά την διαχείριση των Δεδομένων Προσωπικού Χαρακτήρα που αφορούν τους χρήστες. Πράγματι, εξ αντικειμένου, οι εφαρμογές m-Health πρέπει να διαχειριστούν δεδομένα που σχετίζονται με την υγεία, τα οποία θεωρούνται πολύ ευαίσθητα και απολαμβάνουν υψηλότατο βαθμό προστασίας από τους εθνικούς νόμους και τους διεθνείς κανονισμούς, όπως ο ΓΚΠΔ.

Έχοντας ως στόχο την αξιολόγηση της τρέχουσας κατάστασης των εφαρμογών m-Health, όσον αφορά την προστασία των - σχετιζομένων με την υγεία – δεδομένων, αναλύσαμε ένα αντιπροσωπευτικό σύνολο εφαρμογών, προκειμένου να μελετήσουμε τις ποικίλες πρακτικές - πολιτικές Ασφάλειας και Απορρήτου. Η μελέτη μας επισήμανε πληθώρα αδυναμιών των m-Health εφαρμογών. Στο μεγαλύτερο μέρος των εφαρμογών που αναλύσαμε εντοπίσαμε σοβαρά ζητήματα που θέτουν σε κίνδυνο το Απόρρητο και την Ασφάλεια των δεδομένων του χρήστη, παραβιάζοντας έτσι την σχετική νομοθεσία για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα, η οποία έχει θεσπιστεί ακριβώς για να εμποδίσει την ακατάλληλη και ανεξέλεγκτη χρήση, καθώς και την επεξεργασία και την αποκάλυψη ευαίσθητων δεδομένων υγείας σε τρίτους. Σύμφωνα με τα αποτελέσματα της μελέτης μας, ένας ικανός αριθμός δημοφιλών εφαρμογών m-Health θα μπορούσε να παραβιάσει τα δικαιώματα των χρηστών αποκαλύπτοντας δεδομένα όπως: η κατάσταση της υγείας τους, φωτογραφίες, τοποθεσία, ταυτότητα, emails, κτλ.

Μερικά μόνο από τα σημαντικότερα ζητήματα ασφάλειας, τα οποία οι σχεδιαστές – προγραμματιστές m-Health εφαρμογών θα πρέπει να λαμβάνουν υπόψη τους κατά την δημιουργία αυτών, είναι: Η Κρυπτογράφηση, η εκ προοιμίου αίτηση για μετάδοση ευαίσθητων δεδομένων και η ασφάλεια των προγραμματιστών πρακτικών, π.χ. χρήση βιβλιοθηκών τρίτων

υπό προϋποθέσεις. Η δημιουργία και διαχείριση προφίλ χρηστών, ανεξαρτήτως αν πραγματοποιείται για διαφημιστικούς/προωθητικούς σκοπούς, ή για παρακολούθηση της συμπεριφοράς του χρήστη, είναι ένα ακόμη βασικό ζήτημα ασφάλειας, το οποίο πρέπει να λαμβάνεται υπόψη για να διασφαλισθεί η προστασία της Ιδιωτικότητας των χρηστών.

Παρά το γεγονός ότι όλοι οι εμπλεκόμενοι φορείς συμφωνούν ότι η συμμόρφωση με τους ισχύοντες κανονισμούς προστασίας Δεδομένων Προσωπικού Χαρακτήρα παρέχει στους χρήστες Διαφάνεια, όσον αφορά την διαχείριση και επεξεργασία των δεδομένων τους, εξακολουθεί να είναι δύσκολο να επιτευχθεί υψηλός βαθμός λειτουργικότητας των m-Health εφαρμογών, υπό το πρίσμα αυτό. Για παράδειγμα, η επικείμενη εφαρμογή του ΓΚΠΔ, στις 25 Μαΐου 2018, εντός της ΕΕ, αναμένεται να αντιμετωπίσει προκλήσεις τεχνικής φύσεως, όπως: Ο εντοπισμός και η διαγραφή δεδομένων χρήστη που έχουν ήδη διανεμηθεί σε τρίτους, ο σχεδιασμός και η ανάπτυξη εσωτερικών διαδικασιών προς ικανοποίηση των απαιτήσεων του ΓΚΠΔ .

Αν θέλουμε να αποδώσουμε «*τα του Καίσαρος τω Καίσαρι*», οφείλουμε να αναγνωρίσουμε ότι το σημαντικότερο πρόβλημα αυτή τη στιγμή για τους σχεδιαστές και προγραμματιστές m-Health εφαρμογών, δεν είναι ο ΓΚΠΔ αυτό καθεαυτό, αλλά το κενό που υπάρχει ανάμεσα στις νομικές απαιτήσεις του και στο πως οι απαιτήσεις αυτές θα μετατραπούν σε πρακτικές /τεχνικές λύσεις, ώστε να ενσωματωθούν στις εφαρμογές m-Health.

Στο σημείο αυτό εντοπίζεται «*πεδίο δόξης λαμπρό*» για την μελλοντική έρευνα. Πλέον, για τους ερευνητές, έννοιες, που αναφέραμε σε προηγούμενα κεφάλαια, όπως η: «Προστασία των προσωπικών δεδομένων εκ του σχεδιασμού» (Data Protection by Design) και η «εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων» (Data Protection Impact Assessment- DPIA) αποκτούν ιδιαίτερη σημασία, μιας και υπάρχουν εδώ και χρόνια, αλλά, στο πλαίσιο του ΓΚΠΔ αποτελούν πλέον νομική υποχρέωση.

Βιβλιογραφία

[01] A. Blumberg and P. Eckersley, “On locational privacy and how to avoid losing it forever,”2009.

[02] A. Kurtz, H. Gascon, T. Becker, G. Freiling and K. Rieck, “Fingerprinting Mobile Devices Using Personalized Configurations,” in Proceedings on Privacy Enhancing Technologies, 2016.

[03] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea et al., “Smart health: a context-aware health paradigm within smart cities,” IEEE Communications Magazine, vol. 52, no. 8, pp. 74–81, 2014.

[04] A. Solanas, J. H. Weber, A. B. Bener, F. van der Linden, and R. Capilla, “Recent advances in healthcare software: Toward context-aware and smart solutions,” IEEE Software, vol. 34, no. 6, pp. 36–40, 2017.

[05] Blood Glucose Tracker Application (Διαθέσιμη στο: https://play.google.com/store).

[06] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, “Learning internet-of-things security" hands-on"," IEEE Security & Privacy, vol. 14, no. 1, pp. 37–46, 2016.

[07] C. L. Ventola, “Mobile devices and apps for health care professionals: uses and benefits,” PT, vol. 39, no. 5, pp. 356–364, 2014.

[08] C. M. L. Njie, “Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications,” Research Performed For: Privacy Rights Clearinghouse, 2013.

[09] D. Arp, E. Quiring and C. Wressneger, “Privacy Threats through Ultrasonic SideChannels on Mobile Devices,” IEEE Security and Privacy, 2017.

[10] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, “Security concerns in android mhealth apps,” in AMIA Annual Symposium Proceedings, vol. 2014. American Medical Informatics Association, 2014, p. 645.

[11] D. Leibenger, F. Möllers, A. Petrlic, R. Petrlic and C. Sorge, "Privacy Challenges in the Quantified Self Movement – An EU Perspective," in Privacy Enhancing Technologies, 2016.

[12] "Developers and publishers are flocking to the m-Health app market, BI Intelligence, 2016," (Διαθέσιμο στο: http://www.businessinsider.com/developers-andpublishers-are-flocking-to-the-mhealth-app-market-2016-10).

[13] Diabetes Application (Διαθέσιμη στο: https://play.google.com/store).

[14] Diabetes Connect Application (Διαθέσιμη στο: https://play.google.com/store).

[15] Diabetes Diary Application (Διαθέσιμη στο: https://play.google.com/store).

[16] Diabetes Plus Application (Διαθέσιμη στο: https://play.google.com/store).

[17] Dottli Diabetes Made Simple Application (Διαθέσιμη στο: https://play.google.com/store).

[18] D-Partner Application (Διαθέσιμη στο: https://play.google.com/store).

[19] EU GDPR Information Portal, "GDPR Key Changes" (Διαθέσιμο στο: https://www.eugdpr.org/key-changes.html).

[20] EU GDPR Information Portal, "Summary of Articles Contained in the GDPR" (Διαθέσιμο στο: https://www.eugdpr.org/article-summaries.html).

[21] EUR-Lex, Πρόσβαση στο Δίκαιο της Ευρωπαϊκής Ένωσης (Διαθέσιμο στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[22] Glucose Buddy Diabetes Tracker Application (Διαθέσιμη στο: https://play.google.com/store).

[23] J. Achara, G. Acs and C. Castelluccia, "On the Unicity of Smartphone Applications," in 14th ACM CCS Workshop on Privacy in Electronic Society (ACM WPES), 2015.

[24] J. Achara, M. Cunche, V. Roca and A. Francillon, "WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission," in 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), 2014.

[25] J. Brookman, P. Rouge and A. e. a. Alva, "Cross-Device Tracking: Measurement and Disclosures," in Proceedings on Privacy Enhancing Technologies (PETS2017), 2017.

[26] L. Olejnik, G. Acar, C. Castelluccia and C. Diaz, "The leaking battery: A privacy analysis of the HTML5 Battery Status API," 2015.

[27] M. Gadaleta and M. Rossi, "IDNET: Smartphone-based Gait Recognition with Convolutional Neural Networks," 2016.

[28] MedM Diabetes Application (Διαθέσιμη στο: https://play.google.com/store).

[29] My Sugar Diary Diabetes Application (Διαθέσιμη στο: https://play.google.com/store).

[30] N. Bouri and S. Ravi, "Going mobile: how mobile personal health records can improve health care during emergencies," JMIR m-Health and u-Health, vol. 2, no. 1, p. e8, 2014.

[31] N. Vallina-Rodriguez, S. Sundaresan, A. Razaghpanah, R. Nithyanand, M. Allman, C. Kreibich and P. Gill, "Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem," 2016.

[32] National Center for Biotechnology Information (Διαθέσιμο στο: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761894/).

[33] On Track Diabetes Application (Διαθέσιμη στο: https://play.google.com/store).

[34] OPEN EFFECT, "Every Step You Fake. A comparative Analysis of Fitness Tracker Privacy and Security", 2016. (Διαθέσιμο στο: https://citizenlab.org/2016/04/every-step-you-fake-final-report/).

[35] "Overview of the National Laws on Electronic Health Records in the EU Member States – National Report for Greece" (Διαθέσιμο στο: https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_greece_en.pdf).

[36] R. Want, B. N. Schilit, and S. Jenson, “Enabling the internet of things,” Computer, vol. 48, no. 1, pp. 28–35, 2015.

[37] S. Seneviratne, A. Seneviratne, P. Mohapatra and A. Mahanti, “Predicting user traits from a snapshot of apps installed on a smartphone,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 18, no. 2, p. 1–8, 2014.

[38] Special Eurobarometer 431: Data protection, Directorate-General for Communication,2015,” (Διαθέσιμο στο: https://data.europa.eu/euodp/el/data/dataset/S2075_83_1_431_ENG).

[39] Sugar Sense Diabetes Plus Application (Διαθέσιμη στο: https://play.google.com/store).

[40] UK Information Commissioner's Office, “Privacy in mobile apps: guidance for developers,” 2013.

[41] V. Mavroudis, S. Hao, Y. Fratantonio and e. al, “On the Privacy and Security of the Ultrasound Ecosystem.,” in Proceedings on Privacy Enhancing Technologies, 2017.

[42] W. Melicher, M. L. Mazurek, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin and L. Cranor, “Usability and security of text passwords on mobile devices,” in 34th Annual ACM Conference on Human Factors in Computing Systems, 2016.

[43] “WhatsApp says users must be 16 or older to access the app in Europe” (Διαθέσιμο στο: https://www.theverge.com/2018/4/24/17277022/whatsapp-age-limit-access-app-europe).

[44] Y. Zou, J. Zhu and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” in IEEE, 2016.

[45] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen and V. Blondel, “Unique in the Crowd: The Privacy Bounds of Human Mobility,” 2013.

[46] Z. Bauman and D. Lyon, “Liquid Surveillance: A Conversation,” 2013.

[47] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Διαθέσιμη στο: http://www.dpa.gr).

[48] Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα – Ανεξάρτητη Εποπτική Αρχή για την Προστασία του Ατόμου (Διαθέσιμο στο: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/news04_gr/news04_gr?opendocument).

[49] Εθνικό Τυπογραφείο (Διαθέσιμο στο: http://www.et.gr).

[50] Ελληνική Ομοσπονδία για τον Διαβήτη (Διαθέσιμη στο: http://www.elodi.org/).

[51] Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[52] "Η Ευρωπαϊκή ένωση με λίγα λόγια» (Διαθέσιμο στο: https://europa.eu/european-union/about-eu/eu-in-brief_el).

[53] Κανονισμός (ΕΕ) 2013/611 της Επιτροπής της 24ης Ιουνίου 2013 «σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες» (Διαθέσιμος στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[54] 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» (Διαθέσιμος στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[55] Μόνιμη Αντιπροσωπεία της Κυπριακής Δημοκρατίας στην Ευρωπαϊκή Ένωση, «Κύπρος και Ευρωπαϊκή Ένωση», (Διαθέσιμο στο: http://www.mfa.gov.cy/mfa/PermRep/PermRep_Brussels.nsf/page33_gr/page33_gr?OpenDocument).

[56] Νόμος 2472/1997 (ΦΕΚ 50/Α΄/10.04.1997), «Προστασία του Ατόμου από την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και Ενσωμάτωση της Οδηγίας 95/46/ΕΚ στο Ελληνικό Δίκαιο» (Διαθέσιμος στο: http://www.et.gr).

[57] Νόμος 3471/2006 (ΦΕΚ 133/Α΄/28.06.2006), «Προστασία Δεδομένων Προσωπικού Χαρακτήρα και της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών και τροποποίηση του Ν. 2472/97» (Διαθέσιμος στο: http://www.et.gr).

[58] Νόμος4070/2012 (ΦΕΚ 82/Α΄/10.04.2012), «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και Άλλες Διατάξεις» (Διαθέσιμος στο: http://www.et.gr).

[59] 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 και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου» (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[60] Οδηγία 2002/58/ΕΚ για την «Προστασία των Δεδομένων Προσωπικού Χαρακτήρα και την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών» (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[61] Οδηγία 2009/136/ΕΚ «Για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών» (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[62] Οδηγία 95/46/ΕΚ για την «Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και για την Ελεύθερη

Κυκλοφορία των Δεδομένων αυτών» (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[63] Συνθήκη για την Ευρωπαϊκή Ένωση (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

[64] Υπουργείο Εξωτερικών Ελληνικής Δημοκρατίας, «Η Πορεία της Ελλάδας στην Ευρωπαϊκή Ένωση» (Διαθέσιμο στο: https://www.mfa.gr/exoteriki-politiki/i-ellada-stin-ee/i-poreia-tis-elladas-stin-europaiki-enosi.html).

[65] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Διαθέσιμη στο: http://eur-lex.europa.eu/homepage.html?locale=el).

Παράρτημα Α

Κανονισμός (ΕΕ) 2016/679

Το παρόν παράρτημα περιέχει τον πίνακα περιεχομένων του Κανονισμού (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.

Α.1 Περίληψη Άρθρων

Κανονισμός (ΕΕ) 2016/679	
Πίνακας Περιεχομένων	
Κεφάλαιο 1	**Γενικές Διατάξεις**
Άρθρο 1	Αντικείμενο και στόχοι
Άρθρο 2	Ουσιαστικό πεδίο εφαρμογής
Άρθρο 3	Εδαφικό πεδίο εφαρμογής
Άρθρο 4	Ορισμοί
Κεφάλαιο 2	**Αρχές**
Άρθρο 5	Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα
Άρθρο 6	Νομιμότητα της επεξεργασίας

10	
Άρθρο 92	Άσκηση της εξουσιοδότησης
Άρθρο 93	Διαδικασία επιτροπής
Κεφάλαιο 11	**Τελικές διατάξεις**
Άρθρο 94	Κατάργηση της οδηγίας 95/46/ΕΚ
Άρθρο 95	Σχέση με την οδηγία 2002/58/ΕΚ
Άρθρο 96	Σχέση με συμφωνίες που έχουν συναφθεί παλαιότερα
Άρθρο 97	Εκθέσεις της επιτροπής
Άρθρο 98	Επισκόπηση άλλων νομικών πράξεων της Ένωσης για την προστασία των δεδομένων
Άρθρο 99	Έναρξη ισχύος και εφαρμογή

Πίνακας Α1.1: Πίνακας περιεχομένων του Κανονισμού (ΕΕ) 2016/679 [20]