Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Μεταπτυχιακή Διατριβή

Προστασία προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς

Παυλίνα Γεωργίου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Απρίλιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Μεταπτυχιακή Διατριβή

Προστασία προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς

Παυλίνα Γεωργίου

Επιβλέπων Καθηγητής

Κωνσταντίνος Λιμνιώτης

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

στην ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών

του Ανοικτού Πανεπιστημίου Κύπρου.

Απρίλιος 2023

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται την προστασία των προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς.

Παρά τα πλεονεκτήματα που επιφέρει η χρήση τέτοιων εφαρμογών, ταυτόχρονα ανακύπτουν κίνδυνοι και για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων των πολιτών. Κάθε «έξυπνη» εφαρμογή εγείρει, αν δεν σχεδιαστεί σωστά, ζητήματα ιδιωτικότητας – και, μάλιστα, για περιπτώσεις όπως αυτές που μελετώνται στην παρούσα διατριβή, οι συνέπειες μπορεί να είναι ιδιαίτερα σοβαρές λόγω του ότι πρόκειται για ευαίσθητα δεδομένα υγείας.

Η μεθοδολογία που ακολουθήθηκε κατά την συγγραφή της παρούσας διατριβής έγκειται στην δευτερογενή έρευνα, δηλαδή της αναζήτηση επιστημονικών πηγών και εργαλείων με στόχο την επίλυση των ερευνητικών ερωτημάτων.

Αναλύθηκε ο τρόπος λειτουργίας εφαρμογών που σχετίζονται με την υγεία, οι οποίες προωθήθηκαν από κυβερνήσεις χωρών, μέσα από τις βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play και επιπλέον ελέγχθηκαν με το διαδικτυακό εργαλείο Exodus Privacy για την ύπαρξη ιχνηλάτων (trackers) και επικίνδυνα δικαιώματα (high-risk permissions). Τέλος πραγματοποιήθηκε αντιπαραβολή των ευρημάτων έτσι ώστε να δικαιολογηθούν τα permissions που βρέθηκαν, με βάση το privacy policy της εκάστοτε εφαρμογής, υπογραμμίζοντας πολλές σημαντικές και δευτερεύουσες ελλείψεις των εφαρμογών m-health. Ένα μεγάλο μέρος των εφαρμογών που αξιολογήθηκαν διαπιστώθηκε ότι θα μπορούσαν να θέσουν σε κίνδυνο το απόρρητο και την ασφάλεια των χρηστών παραβιάζοντας τους ευαίσθητους κανονισμούς προστασίας δεδομένων που έχουν τεθεί για την πρόληψη της ακατάλληλης και ανεξέλεγκτης χρήσης, επεξεργασίας και αποκάλυψης δεδομένων υγείας σε τρίτους.

Summary

This thesis deals with the protection of personal data in Android applications related to health by government agencies.

Despite the advantages brought about by the use of such applications, at the same time risks also arise for the privacy and protection of personal data of citizens. Any “smart” application raises, if not designed properly, privacy issues – and indeed, for cases like those studied in this thesis, the consequences can be particularly serious due to the sensitive health data involved.

The methodology followed during the writing of this thesis lies in secondary research, that is, the search for scientific sources and tools with the aim of solving the research questions.

The operation of health-related applications, which were promoted by country governments, was analyzed through the ratings and evaluations of the Google Play website and additionally checked with the online tool Exodus Privacy for the existence of trackers and dangerous rights (high- risk permissions). Finally, a comparison of the findings was carried out in order to justify the permissions found, based on the privacy policy of each application, highlighting many important and secondary shortcomings of m-health applications. A large proportion of the apps assessed were found to be potentially compromising user privacy and security by violating sensitive data protection regulations set to prevent the inappropriate and uncontrolled use, processing and disclosure of health data to third parties.

Ευχαριστίες

Με την παρούσα δήλωση τελειώνει η συμμετοχή μου στο Μεταπτυχιακό Πρόγραμμα Ασφάλεια Υπολογιστών και Δικτύων της Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστήμιο Κύπρου.

Με την φοίτησή μου στο παρόν μεταπτυχιακό, το οποίο παρέχει ανώτατη ποιότητα σπουδών, απόκτησα νέες γνώσεις της εποχής μου που θα με βοηθήσουν να είμαι καλύτερη στην εργασία μου αλλά και στην ζωή μου γενικότερα.

Καθ' όλη τη διάρκεια της συγγραφής της διατριβής αυτής έλαβα μεγάλη υποστήριξη και βοήθεια.

Αρχικά θα ήθελα να ευχαριστήσω από την καρδιά μου τον κο Κωνσταντίνο Λιμνιώτη, καθηγητή μου, εισηγητή και επιβλέποντα του θέματος της διατριβής μου: «Προστασία προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς». Η τεχνογνωσία ήταν πολύτιμη στη διατύπωση των ερευνητικών ερωτημάτων και της μεθοδολογίας. Τα ευφυή και άμεσα σχόλια με ώθησαν να αποζητήσω, να καταγράψω και να έχω δημιουργικό στοχασμό, συστατικά που ώθησαν το παρόν πόνημα σε υψηλότερο επίπεδο.

Θα ήθελα επιπροσθέτως να ευχαριστήσω όλους τους καθηγητές μου, ξεχωριστά, για την πολύτιμη καθοδήγησή τους καθ' όλη τη διάρκεια των σπουδών μου στο παρόν Μεταπτυχιακό. Μου παρείχαν τα εργαλεία που χρειαζόμουν για να επιλέξω τη σωστή κατεύθυνση στον τρόπο οργάνωσης και ανάλυσης της γνώσης και να ολοκληρώσω με επιτυχία τις σπουδές μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, τους γονείς μου και τον παππού μου Αρίσταρχο που με στήριξε στην προσπάθεια μου αυτή.

Παυλίνα Γεωργίου

Περιεχόμενα

Κατάλογος Εικόνων

Κεφάλαιο 1
Εισαγωγή

Στο πρώτο κεφάλαιο παρουσιάζονται γενικά στοιχεία για το θέμα της προστασίας προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς, ο σκοπός της έρευνας, τα βασικά ερευνητικά ερωτήματα και τέλος η αναγκαιότητα και σπουδαιότητα έρευνας.

1.1 Γενικά Στοιχεία

Η ραγδαία τεχνολογική ανάπτυξη και η εισδοχή της στην καθημερινότητα των ανθρώπων έχει δημιουργήσει την ανάγκη για ψηφιοποίηση των μέχρι τώρα έντυπων εγγράφων, αλλά και την αυτοματοποίηση πολλών επεξεργασιών, μέσω ηλεκτρονικών εφαρμογών. Η ψηφιοποίηση αυτή δεν θα μπορούσε βέβαια να αποφευχθεί και στον τομέα της υγείας αφού οι πολίτες κάθε κράτους καλούνται να διαθέτουν συγκεκριμένα έγγραφα τα οποία τους δίνουν την δυνατότητα να χρησιμοποιούν τις παροχές υγείας των εκάστοτε χωρών. Έχουν δημιουργηθεί από συγκεκριμένους φορείς των διαφόρων χωρών συγκεκριμένες εφαρμογές για την αποθήκευση αλλά και την κοινοποίηση -μεταξύ των αρμοδίων αρχών αλλά και των ιατρών- αυτών των εγγράφων.

Από την άλλη την τελευταία διετία η πανδημία της νόσου του κορονοϊού που κλόνισε τον πλανήτη, μας έχει φέρει αντιμέτωπους με νέα προβλήματα τα οποία καλούμαστε να ξεπεράσουμε. Ένα τέτοιο πρόβλημα αντιμετώπισαν πολλές κυβερνήσεις αφού κλήθηκαν να βρουν τρόπους να ελέγχουν τον κάθε πολίτη για το αν ή όχι κατέχει πιστοποιητικό εμβολιασμού, νόσησης, είτε κάποιο αρνητικό τεστ. Δημιούργησαν λοιπόν και προώθησαν «έξυπνες» εφαρμογές με την χρήση των οποίων οι πολίτες της εκάστοτε χώρας μπορούν είτε να αποθηκεύσουν -το λεγόμενο- Safe Pass τους είτε να σκανάρουν κατά πόσο κάποιο Safe Pass είναι έγκυρο ή όχι. Παράλληλα, αναπτύσσονται και εφαρμογές στο πλαίσιο του ηλεκτρονικού φακέλου υγείας, έτσι ώστε ο κάθε πολίτης να έχει ηλεκτρονικά πρόσβαση στα συνολικά ιατρικά του δεδομένα, ενώ το ίδιο θα μπορεί να γίνεται – εφόσον ο χρήστης

συναινεί – και από παρέχοντες υπηρεσίες υγείας. Μάλιστα, η Ευρωπαϊκή Επιτροπή από το 2022 έχει πρόταση Κανονισμού αναφορικά με το διαμοιρασμό δεδομένων υγείας (European Health Data Space), τόσο για σκοπούς παροχής εξατομικευμένων υπηρεσιών υγείας όσο και για δευτερογενείς σκοπούς όπως επιστημονικούς, στατιστικούς, λήψη αποφάσεων για τη δημόσια υγεία, για επάρκεια φαρμάκων κ.α. Στην εν λόγω πρόταση Κανονισμού γίνεται ρητή αναφορά στο ότι και δεδομένα «έξυπνων» εφαρμογών υγείας θα μπορούν, υπό προϋποθέσεις, να διαμοιράζονται με τρίτους.

Παρά τα πλεονεκτήματα που επιφέρει η χρήση τέτοιων εφαρμογών, ταυτόχρονα ανακύπτουν κίνδυνοι και για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων των πολιτών. Κάθε «έξυπνη» εφαρμογή εγείρει, αν δεν σχεδιαστεί σωστά, ζητήματα ιδιωτικότητας – και, μάλιστα, για περιπτώσεις όπως αυτές που μελετώνται στην παρούσα διατριβή, οι συνέπειες μπορεί να είναι ιδιαίτερα σοβαρές λόγω του ότι πρόκειται για ευαίσθητα δεδομένα υγείας.

Στην παρούσα διπλωματική θα εντοπιστεί συγκεκριμένος αριθμός γνωστών εφαρμογών τις οποίες οι κυβερνήσεις χωρών ιδίως της Ευρώπης διαθέτουν στους πολίτες τους. Στη συνέχεια θα γίνει ανάλυση αυτών των εφαρμογών τόσο ως προς ζητήματα ασφάλειας όσο και ως προς ζητήματα ιδιωτικότητας και προστασίας δεδομένων. Δεδομένου ότι η Ευρωπαϊκή Ένωση έχει κοινό γενικό νομικό πλαίσιο για την προστασία προσωπικών δεδομένων, θα γίνει αντιπαραβολή και με κάποιες ενδεικτικές εφαρμογές χωρών εκτός Ευρώπης.

1.2 Σκοπός έρευνας

Σκοπός της έρευνας είναι η μελέτη των διαφόρων εφαρμογών που αφορούν στον τομέα της υγείας και οι οποίες παρέχονται από δημόσιους φορείς, ως προς την λειτουργία τους όσον αφορά την ασφάλεια, την ιδιωτικότητα αλλά και την προστασία των δεδομένων των χρηστών. Στο πλαίσιο αυτό θα δοθεί ειδικότερα έμφαση στον πιθανό εντοπισμό λανθασμένων τρόπων λειτουργίας των συγκεκριμένων εφαρμογών, σε τυχόν ελλιπή ενημέρωση ή και μη ορθή σχεδίασή τους όσον αφορά την ιδιωτικότητα αλλά και την προστασία των δεδομένων.

1.3 Βασικά Ερευνητικά Ερωτήματα

Τα βασικά ερευνητικά ερωτήματα της παρούσης διατριβής είναι τα εξής:

1. Κατά πόσο οι εφαρμογές υγείας που προωθούν οι κυβερνήσεις στους πολίτες τους αναπτύσσονται σύμφωνα με τις αρχές «data protection by design» και «data protection by default».
2. Αν υπάρχουν διαφορές - και, εάν ναι, πού αυτές έγκεινται - στις προσεγγίσεις που ακολουθούν οι διάφορες κυβερνήσεις.
3. Αν η λειτουργία των εν λόγω εφαρμογών είναι διαφανής στους πολίτες.
4. Κατά πόσο τα δεδομένα που εισάγουν οι χρήστες/ασθενείς στις εφαρμογές υγείας προωθούμενες από την κυβέρνηση είναι προσβάσιμα αυστηρά και μόνο από τα άμεσα ενδιαφερόμενα μέλη (πχ. Ιατρούς, φορείς υγείας κτλ.).

1.4 Αναγκαιότητα και σπουδαιότητα έρευνας

Η ψηφιοποίηση των υπηρεσιών υγείας είναι διαρκώς εξελισσόμενη, με την τάση να γίνεται ανταλλαγή δεδομένων υγείας μεταξύ διαφόρων συστημάτων/πλατφορμών όχι μόνο για σκοπούς παροχής υπηρεσιών υγείας αλλά και για άλλους σκοπούς όπως η χάραξη δημοσίων πολιτικών και η λήψη στρατηγικών αποφάσεων από αρμόδιους δημόσιους φορείς αναφορικά με τη Δημόσια Υγεία, όπως επίσης και για ερευνητικούς σκοπούς. Στο πλαίσιο αυτό, και στην εποχή των δεδομένων μεγάλου όγκου (Big Data), οι χρήστες οι ίδιοι «τροφοδοτούν» τα συστήματα αυτά με δεδομένα τους, πολλές φορές μέσα από «έξυπνες εφαρμογές». Ωστόσο, όλο αυτό το οικοσύστημα εγείρει ταυτόχρονα και σοβαρούς κινδύνους ιδιωτικότητας και προστασίας δεδομένων. Ειδικότερα, σε ευρωπαϊκό επίπεδο, αναφορικά με την προαναφερθείσα πρόταση Κανονισμού της Ε.Ε. για ένα περιβάλλον ανταλλαγής δεδομένων υγείας (Health Data Space), αρμόδιοι φορείς προστασίας δεδομένων έχουν εκφράσει τη γνώμη ότι σημαντικές τροποποιήσεις πρέπει να γίνουν στο σχέδιο αυτό προκειμένου να παρέχονται εχέγγυα για την προστασία των προσωπικών δεδομένων των χρηστών (European Union/EDPB-EDPS, 2022). Στο πλαίσιο αυτό, οι «έξυπνες» εφαρμογές που επεξεργάζονται δεδομένα υγείας αποκτούν ιδιαίτερη σημασία λόγω του γεγονότος ότι όλες οι «έξυπνες» εφαρμογές, ανεξαρτήτως του είδους των δεδομένων που επεξεργάζονται, εγγενώς χαρακτηρίζονται από διάφορα «αδύναμα» σημεία ως προς την προστασία προσωπικών δεδομένων. Εφόσον λοιπόν πρόκειται για δεδομένα υγείας, οι κίνδυνοι από τη μη ορθή χρήση των δεδομένων αυτών επιτείνονται. Αυτό μάλιστα επιτείνεται σε περιπτώσεις που οι εφαρμογές προσφέρονται από Δημόσιους φορείς και έχουν υποχρεωτικό χαρακτήρα.

1.5 Μεθοδολογία έρευνας

Η μεθοδολογία που ακολουθήθηκε κατά την συγγραφή της παρούσας διατριβής έγκειται στην δευτερογενή έρευνα, δηλαδή της αναζήτηση επιστημονικών πηγών και εργαλείων με στόχο την επίλυση των ερευνητικών ερωτημάτων.

Αναλύθηκε ο τρόπος λειτουργίας εφαρμογών που σχετίζονται με την υγεία, οι οποίες προωθήθηκαν από κυβερνήσεις χωρών, μέσα από τις βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play και επιπλέον ελέγχθηκαν με το διαδικτυακό εργαλείο Exodus Privacy για την ύπαρξη ιχνηλάτων (trackers) και επικίνδυνα δικαιώματα (high-risk permissions). Τέλος πραγματοποιήθηκε αντιπαραβολή των ευρημάτων έτσι ώστε να δικαιολογηθούν τα permissions που βρέθηκαν, με βάση το privacy policy της εκάστοτε εφαρμογής.

1.6 Δομή διατριβής

Η δομή της παρούσας διατριβής έχει ως εξής:

Αρχικά στη 1η ενότητα την «Εισαγωγή», παρουσιάζονται γενικά στοιχεία του θέματος, ο σκοπός της έρευνας, τα βασικά ερευνητικά ερωτήματα που δημιουργούνται, η αναγκαιότητα και η σπουδαιότητα έρευνας και τέλος η μεθοδολογία και η δομή της διατριβής.

Στην 2η ενότητα της βιβλιογραφικής ανασκόπησης, πραγματοποιείται έρευνα επιστημονικών πηγών για το θέμα της προστασίας προσωπικών δεδομένων σε εφαρμογές Android. Παρέχεται μια επισκόπηση της τρέχουσας γνώσης, επιτρέποντας τον εντοπισμό σχετικών θεωριών, μεθόδων και κενών στην υπάρχουσα έρευνα.

Στην 3η ενότητα για την Προστασία προσωπικών δεδομένων, αρχικά αποσαφηνίζονται σχετικές έννοιες, έπειτα καταγράφεται η Ευρωπαϊκή Νομοθεσία, η Κυπριακή και η Ελληνική Νομοθεσία για τα προσωπικά δεδομένα.

Στην 4η ενότητα με θέμα τις εφαρμογές Android και προστασία προσωπικών δεδομένων, παρουσιάζεται το λειτουργικό Android και τα χαρακτηριστικά του, οι εφαρμογές του Android και τέλος η ασφάλεια και ιδιωτικότητα (τεχνικά χαρακτηριστικά ασφαλείας, συνήθεις απειλές για την ασφάλεια, εντοπισμός τοποθεσίας, ιχνηλάτες (trackers), περαιτέρω δικλείδες ασφαλείας).

Στην 5η ενότητα με θέμα την σχεδιαστική προσέγγιση «data protection by design» και «data protection by default» των εφαρμογών Android: υγείας από κρατικούς φορείς, καταγράφεται το Data Protection by Design εφαρμογών Android υγείας από κρατικούς φορείς (κανονισμοί απορρήτου και προστασίας δεδομένων για τις εφαρμογές mHealth στην ΕΕ, Privacy by Design σε εφαρμογές Mobile Healthcare, και το Data Protection By Default εφαρμογών Android υγείας από κρατικούς φορείς (η εμπειρία από τις εφαρμογές ιχνηλάτησης COVID-19 ασθενών, Privacy-by-design στην αντιμετώπιση κινδύνων).

Στην 6η ενότητα παρουσιάζονται οι εφαρμογές Android: Coronapas της Δανίας, Passe Covid της Πορτογαλίας, CovPass της Γερμανίας, CovScan Cyprus και CovPass Cyprus της Κυπριακής Κυβέρνησης, Covid Free GR και MyHealth της Ελληνικής Δημοκρατίας, COVID Alert NJ από το Υπουργείο Υγείας του Νιου Τζέρσεϋ (DOH), WHO Info και OpenWHO του Παγκόσμιου Οργανισμού Υγείας / ΠΟΥ.

Στην 7η ενότητα παρουσιάζονται τα συμπεράσματα για την προστασία προσωπικών δεδομένων σε εφαρμογές Android που αφορούν την υγεία από κρατικούς φορείς.

Κεφάλαιο 2
Ανασκόπηση Βιβλιογραφίας

Στο παρόν κεφάλαιο της βιβλιογραφικής ανασκόπησης πραγματοποιείται έρευνα επιστημονικών πηγών για το θέμα της προστασίας προσωπικών δεδομένων σε εφαρμογές Android. Παρέχεται μια επισκόπηση της τρέχουσας γνώσης, επιτρέποντας τον εντοπισμό σχετικών θεωριών, μεθόδων και κενών στην υπάρχουσα έρευνα.

2.1 Ανασκόπηση Βιβλιογραφίας

Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας, η εφαρμογή της ψηφιακής υγείας μέσω της ανταλλαγής πληροφοριών και δεδομένων μεταξύ ασθενών και παρόχων υπηρεσιών υγείας, μπορεί να έχει οφέλη για το επίπεδο υγείας των πολιτών και ολόκληρης της κοινωνίας χάρη στη βελτίωση της προσβασιμότητας και της ποιότητας της περίθαλψης και στην ενίσχυση της αποτελεσματικότητας του τομέα της υγείας (World Health Organization, 2012).

Σε πολλές χώρες ανά τον κόσμο οι κυβερνήσεις προσπαθώντας να συμβαδίσουν με την συνεχώς αναπτυσσόμενη τεχνολογία και με στόχο την πιο εύκολη και αποτελεσματικότερη παροχή υπηρεσιών υγείας στους πολίτες τους προχώρησαν στην δημιουργία εφαρμογών οι οποίες προσφέρουν την ευκαιρία στους πολίτες της κάθε χώρας να χρησιμοποιήσει το σύστημα υγείας έχοντας πρόσβαση σε αποτελέσματα εξετάσεών, συνταγογραφήσεις, τη δυνατότητα διευθέτησης ραντεβού με ιατρό και άλλα.

Όμως κάθε διαδικασία εξέλιξης και προόδου έχει προκλήσεις. Στην προκειμένη περίπτωση οι κυβερνήσεις κλήθηκαν να αντιμετωπίσουν μια αρκετά δύσκολη πρόκληση. Αυτή της ασφάλειας και προστασίας των δεδομένων των πολιτών που χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες υγείας που προσφέρονται μέσω των εφαρμογών που προωθούν. Οι κυβερνήσεις καλούνται να διαβεβαιώσουν τους πολίτες ότι η ιδιωτικότητά

τους προστατεύεται και οι πληροφορίες τους δεν θα πωληθούν σε τρίτους (Kushchu & Kuscu, 2004).

Η πολιτική απορρήτου (privacy policy) που παρέχεται από στην κάθε εφαρμογή οφείλει να είναι διαθέσιμη ευχερώς στον χρήστη πριν την εγκατάσταση ή χρήση της εκάστοτε εφαρμογής. Δεδομένου ότι όλο και περισσότεροι άνθρωποι χρησιμοποιούν εφαρμογές στα κινητά τους τηλέφωνα και φορητές συσκευές για να μετρήσουν την υγεία τους, είναι σημαντικό να γίνει έρευνα σε αυτόν τον τομέα. Σήμερα, το απόρρητο, και λόγω της συνεχής εξωστρέφειας των ανθρώπων από την χρήση μέσων κοινωνικής δικτύωσης αλλά και πλειάδας εφαρμογών (smartphone), είναι μια δύσκολη διεργασία. Αυτός μπορεί να είναι ο λόγος που όλο και περισσότερες εταιρείες χρησιμοποιούν το απόρρητο τόσο στα επιχειρηματικά τους μοντέλα όσο και ως εργαλείο μάρκετινγκ. Αυτό εγείρει το ερώτημα εάν οι άνθρωποι δίνουν πραγματικά ενημερωμένη συγκατάθεση για τις πολιτικές απορρήτου, καθώς φαίνεται να βασίζονται σε δηλώσεις μάρκετινγκ αντί να διαβάζουν οι ίδιοι τις πραγματικές πολιτικές απορρήτου. Σύμφωνα με έρευνα των Mulder & Tudorica, (2020), η οποία ανέλυσε διάφορες εφαρμογές που κινούνται στον τομέα της υγείας μόνο μία στις οκτώ εφαρμογές έχει ξεχωριστή πολιτική απορρήτου που προσφέρει στον χρήστη πριν από τη λήψη ή τη χρήση της εφαρμογής. Αυτή η έρευνα έδειξε ότι υπάρχει ένα χάσμα μεταξύ της νομοθεσίας περί προστασίας δεδομένων στην Ευρώπη και της πρακτικής πραγματικότητας. Αφού συνέκριναν τις πολιτικές απορρήτου τριών εμπορικών εφαρμογών υγείας και φορητών συσκευών με τις διατάξεις του GDPR, συμπεράναν ότι αυτές οι πολιτικές απορρήτου είναι ασαφείς σχετικά με τις δραστηριότητες επεξεργασίας γενικά. Είναι ευθύνη αυτών των εταιρειών να προστατεύουν το απόρρητο των χρηστών τους. Ενώ εκ πρώτης όψεως οι πολιτικές φαίνονται καλά διατυπωμένες και η δήλωση μάρκετινγκ δίνει την εντύπωση ότι το απόρρητο είναι σημαντικό, μια προσεκτική ανάλυση αυτών των τριών πολιτικών έδειξε ότι είναι ασαφείς σχετικά με τους σκοπούς της επεξεργασίας, το πόσα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία, πού /πώς γίνεται η επεξεργασία των δεδομένων και σε ποιους κοινοποιούνται τα δεδομένα. Λαμβάνοντας αυτό υπόψη, σε συνδυασμό με το γεγονός ότι οι άνθρωποι συχνά δεν διαβάζουν τις πολιτικές απορρήτου ή/και επιλέγουν την ευκολία έναντι του απορρήτου, είναι κατά τη γνώμη τους καθήκον των εποπτικών αρχών να παρακολουθούν τη συμμόρφωση αυτών των εταιρειών με τον GDPR. Αυτό μπορεί να γίνει με τη συνεργασία μεταξύ εθνικών και ευρωπαϊκών εποπτικών αρχών. Ωστόσο, οι προκλήσεις δεν μπορούν να αντιμετωπιστούν μόνο με νομικά μέσα και με την επιβολή τους από τις εποπτικές αρχές.

Είναι επίσης σε μεγάλο βαθμό μια κοινωνική πρόκληση που θα μπορούσαν να αντιμετωπιστούν από κοινωνικές οργανώσεις (όπως οργανώσεις ασθενών, ενώσεις καταναλωτών κ.λπ.) μέσω διαφόρων εκστρατειών. Με αυτόν τον τρόπο μπορεί πραγματικά να επιτευχθεί η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων σε σχέση με τη διασυνοριακή επεξεργασία δεδομένων υγείας (Mulder & Tudorica, 2020).

Οι πρόσφατες εξελίξεις στο υλικό και στις τηλεπικοινωνίες επέτρεψαν την ανάπτυξη κινητών συσκευών χαμηλού κόστους εξοπλισμένων με μια ποικιλία αισθητήρων. Ως αποτέλεσμα, οι νέες λειτουργίες, που ενισχύονται από τις αναδυόμενες πλατφόρμες κινητής τηλεφωνίας, επιτρέπουν σε εκατομμύρια εφαρμογές να εκμεταλλεύονται τεράστιες ποσότητες δεδομένων. Ακολουθώντας αυτή την τάση, οι εφαρμογές υγείας για κινητές συσκευές συλλέγουν πληροφορίες σχετικά με την υγεία των χρηστών για να τους βοηθήσουν να κατανοήσουν καλύτερα την κατάσταση της υγείας τους και να προάγουν τη συνολική ευημερία τους. Ωστόσο, οι πληροφορίες που σχετίζονται με την υγεία από τη φύση τους και από το νόμο θεωρούνται ευαίσθητες και, ως εκ τούτου, η επαρκής προστασία τους είναι ουσιαστικής σημασίας. Στην έρευνά τους οι Papageorgiou et al., 2018) παρέχουν μια εις βάθος ανάλυση ασφάλειας και απορρήτου μερικών από τις πιο δημοφιλείς εφαρμογές υγείας για κινητές συσκευές δωρεάν λογισμικού. Έχουν πραγματοποιήσει τόσο στατική όσο και δυναμική ανάλυση επιλεγμένων εφαρμογών υγείας για κινητά, μαζί με προσαρμοσμένη δοκιμή των λειτουργιών κάθε εφαρμογής. Οι μακροπρόθεσμες αναλύσεις του κύκλου ζωής των εφαρμογών που εξετάζονται και η γενική διαδικασία ελέγχου συμμόρφωσης με τον κανονισμό προστασίας δεδομένων είναι μοναδικά χαρακτηριστικά της εργασίας τους. Τα ευρήματά τους αποκαλύπτουν ότι η πλειονότητα των εφαρμογών που αναλύθηκαν δεν ακολουθούν γνωστές πρακτικές και οδηγίες, ούτε καν νομικούς περιορισμούς που επιβάλλονται από τους σύγχρονους κανονισμούς προστασίας δεδομένων, θέτοντας έτσι σε κίνδυνο το απόρρητο εκατομμυρίων χρηστών (Papageorgiou, και συν., 2018).

Οι Mia, και συν., (2022) παρουσίασαν συγκριτική μελέτη για την αξιολόγηση τεχνικών διασφαλίσεων HIPAA για εφαρμογές android mHealth. Η προστασία των προσωπικών αρχείων υγείας γίνεται ολοένα και πιο σημαντική καθώς όλο και περισσότεροι άνθρωποι χρησιμοποιούν εφαρμογές Mobile Health (εφαρμογές mHealth) για να βελτιώσουν τα αποτελέσματα της υγείας τους. Αυτές οι εφαρμογές mHealth επιτρέπουν στους καταναλωτές να παρακολουθούν τα προβλήματα υγείας τους, να αποθηκεύουν, να

διαχειρίζονται και να μοιράζονται αρχεία υγείας, ιατρικές καταστάσεις, θεραπεία και φάρμακα. Με την αύξηση της προσβασιμότητας και της χρηστικότητας των εφαρμογών mHealth, είναι σημαντικό να δημιουργούνται, να λαμβάνονται, να διατηρούνται ή να μεταδίδονται προστατευμένες πληροφορίες υγείας (protected health information / PHI) για λογαριασμό μιας δημόσιας οντότητας ή άλλου επιχειρηματικού συνεργάτη. Ο νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (Health Insurance Portability and Accountability Act / HIPAA) στις ΗΠΑ παρέχει οδηγίες στους προγραμματιστές εφαρμογών, έτσι ώστε οι εφαρμογές να πρέπει να συμμορφώνονται με τις απαιτούμενες τεχνικές διασφαλίσεις διευθυνσιοδότησης. Ωστόσο, οι περισσότεροι προγραμματιστές εφαρμογών για κινητά, συμπεριλαμβανομένων των εφαρμογών mHealth, δεν γνωρίζουν τους κανονισμούς ασφάλειας και απορρήτου HIPAA. Ως εκ τούτου, προέκυψε μια ερευνητική ευκαιρία για την ανάπτυξη ενός αναλυτικού πλαισίου για να βοηθήσει τον εκάστοτε προγραμματιστή να διατηρήσει έναν ασφαλή και συμβατό με το HIPAA πηγαίο κώδικα και να αυξήσει την ευαισθητοποίηση των καταναλωτών σχετικά με το απόρρητο και την ασφάλεια των ευαίσθητων και προσωπικών πληροφοριών υγείας. Προτείνεται μια ανάλυση / πλαίσιο πηγαίου κώδικα Android που αξιολογεί δώδεκα τεχνικές διασφαλίσεις HIPAA για να ελέγξει εάν μια εφαρμογή mHealth είναι συμβατή με το HIPAA ή όχι. Οι εφαρμοζόμενοι αλγόριθμοι μετα-ανάλυσης και ροής δεδομένων εντοπίζουν αποτελεσματικά τα χαρακτηριστικά κινδύνου και ασφάλειας των εφαρμογών mHealth που παραβιάζουν τους κανονισμούς HIPAA. Επιπλέον, αντιμετωπίστηκε από τους ερευνητές έλεγχος επιπέδου API για ασφαλή επικοινωνία δεδομένων που επιβάλλεται από πρόσφατες οδηγίες CMS μεταξύ εφαρμογών υγείας τρίτων για κινητά και συστήματα EHR (Electronic Health Records / Ηλεκτρονικός Φάκελος Ασθενούς). Πειραματικά, έχει αναπτυχθεί ένα διαδικτυακό εργαλείο για την αξιολόγηση της αποτελεσματικότητας των τεχνικών ανάλυσης και των αλγορίθμων. Ερευνήθηκαν 200 κορυφαίες δημοφιλείς εφαρμογές Android της κατηγορίας: Ιατρική, Υγεία και Γυμναστική που συλλέχθηκαν από το Google Play Store. Εντοπίστηκε από τη συγκριτική ανάλυση των αποτελεσμάτων αξιολόγησης των κανόνων HIPAA ότι η εξουσιοδότηση πρόσβασης σε ευαίσθητους πόρους, η κρυπτογράφηση-αποκρυπτογράφηση δεδομένων και η ασφάλεια μετάδοσης δεδομένων είναι τα πιο ευάλωτα χαρακτηριστικά των εφαρμογών που ερευνήθηκαν. Παράχθηκαν συστάσεις στους προγραμματιστές εφαρμογών σχετικά με το πιο συνηθισμένο λάθος που έγινε κατά τη στιγμή της ανάπτυξης της εφαρμογής και πώς να αποφευχθούν αυτά τα λάθη για την εφαρμογή ασφαλών και συμβατών με HIPAA εφαρμογών. Το προτεινόμενο

πλαίσιο δίνει τη δυνατότητα να αναπτυχθεί ένα IDE πρόσθετο για προγραμματιστές εφαρμογών mHealth και μια διεπαφή βασισμένη στον ιστό για τους καταναλωτές εφαρμογών mHealth (Mia, και συν., 2022).

Ένα πλαίσιο ασφαλείας για εφαρμογές mHealth στην πλατφόρμα Android μελέτησαν οι Hussain, και συν., (2018). Οι εφαρμογές Mobile Health (mHealth) είναι εύκολα προσβάσιμες στους μέσους χρήστες κινητών συσκευών και παρά τις δυνατότητες των εφαρμογών mHealth να βελτιώσουν τη διαθεσιμότητα, την οικονομική προσιτότητα και την αποτελεσματικότητα της παροχής υπηρεσιών υγειονομικής περίθαλψης, χειρίζονται ευαίσθητα ιατρικά δεδομένα και ως εκ τούτου ενδέχεται να εγκυμονούν σημαντικούς κινδύνους για την ασφάλεια και το απόρρητο των χρηστών τους. Οι προγραμματιστές εφαρμογών είναι συνήθως άγνωστοι και οι χρήστες δεν γνωρίζουν πώς γίνεται η διαχείριση και χρήση των δεδομένων τους. Αυτό συνδυάζεται με την εμφάνιση νέων απειλών λόγω της ανεπάρκειας στην ανάπτυξη εφαρμογών ή των ασαφειών σχεδιασμού των σημερινών λειτουργικών συστημάτων για κινητά τηλέφωνα. Πολλά λειτουργικά συστήματα για κινητά τηλέφωνα είναι διαθέσιμα στην αγορά, αλλά η πλατφόρμα Android έχει κερδίσει τη μεγαλύτερη δημοτικότητα. Ωστόσο, το μοντέλο ασφαλείας Android δεν μπορεί να εξασφαλίσει πλήρως το απόρρητο και την ασφάλεια των δεδομένων των χρηστών, συμπεριλαμβανομένων των δεδομένων των εφαρμογών mHealth. Παρά τους μηχανισμούς ασφαλείας που παρέχονται από το Android, όπως οι άδειες και το sandboxing, οι εφαρμογές mHealth εξακολουθούν να μαστίζονται από σοβαρά ζητήματα απορρήτου και ασφάλειας. Αυτά τα ζητήματα ασφάλειας πρέπει να αντιμετωπιστούν προκειμένου να βελτιωθεί η αποδοχή των εφαρμογών mHealth από τους χρήστες και η αποτελεσματικότητα των εφαρμογών mHealth στα συστήματα υγειονομικής περίθαλψης. Το επίκεντρο της έρευνας των Hussain, και συν., (2018) είναι η ασφάλεια των εφαρμογών mHealth και ο κύριος στόχος τους είναι να προτείνουν ένα συνεκτικό, πρακτικό και αποτελεσματικό πλαίσιο για τη βελτίωση της ασφάλειας των ιατρικών δεδομένων που σχετίζονται με τις εφαρμογές Android mHealth, καθώς και την προστασία του απορρήτου των χρηστών τους. Το προτεινόμενο πλαίσιο παρέχει την επιδιωκόμενη προστασία του κυρίως μέσω ενός συνόλου ελέγχων ασφαλείας και πολιτικών που διασφαλίζουν προστασία από παραδοσιακές, καθώς και πρόσφατα δημοσιευμένες απειλές για εφαρμογές mHealth. Η σχεδίαση του πλαισίου περιλαμβάνει δύο επίπεδα: ένα επίπεδο μονάδας ασφαλείας (Security Module Layer / SML) που υλοποιεί τις μονάδες ελέγχου ασφαλείας και ένα επίπεδο διεπαφής συστήματος (System Interface Layer / SIL) που διασυνδέει τη SML με το λειτουργικό σύστημα Android. Η SML

επιβάλλει πολιτικές ασφάλειας και απορρήτου σε διαφορετικά επίπεδα πλατφόρμας Android μέσω του SIL. Το προτεινόμενο πλαίσιο επικυρώνεται μέσω μιας πρωτότυπης υλοποίησης σε πραγματικές συσκευές Android για να δείξει την πρακτικότητά του και να αξιολογήσει την απόδοσή του. Το πλαίσιο αξιολογείται ως προς την αποτελεσματικότητα και την αποδοτικότητα. Η αποτελεσματικότητα αξιολογείται με την επίδειξη της απόδοσης του πλαισίου έναντι ενός επιλεγμένου συνόλου επιθέσεων, ενώ η απόδοση αξιολογείται συγκρίνοντας τα γενικά έξοδα απόδοσης όσον αφορά την κατανάλωση ενέργειας, τη μνήμη και τη χρήση της CPU, με την απόδοση μιας κύριας, έκδοσης του Android. Τα αποτελέσματα των πειραματικών αξιολογήσεων έδειξαν ότι το προτεινόμενο πλαίσιο μπορεί να προστατεύσει επιτυχώς τις εφαρμογές mHealth από ένα ευρύ φάσμα επιθέσεων με αμελητέα επιβάρυνση, επομένως είναι αποτελεσματικό και πρακτικό (Hussain, και συν., 2018).

Εν συνεχεία οι Fan, και συν., (2020) παρέθεσαν μια εμπειρική αξιολόγηση των παραβιάσεων της συμμόρφωσης με τον GDPR στις εφαρμογές mHealth Android. Ο σκοπός του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) είναι να παρέχει βελτιωμένη προστασία της ιδιωτικής ζωής. Εάν μια εφαρμογή ελέγχει προσωπικά δεδομένα από χρήστες, πρέπει να συμμορφώνεται με τον GDPR. Ωστόσο, το GDPR παραθέτει γενικούς κανόνες αντί για ακριβείς οδηγίες βήμα προς βήμα σχετικά με τον τρόπο ανάπτυξης μιας εφαρμογής που πληροί τις απαιτήσεις. Επομένως, ενδέχεται να υπάρχουν παραβιάσεις συμμόρφωσης με τον GDPR σε υπάρχουσες εφαρμογές, οι οποίες θα αποτελούσαν σοβαρές απειλές για το απόρρητο για τους χρήστες των εφαρμογών. Στην έρευνά τους οι Fan, και συν., (2020) , λαμβάνουν τις εφαρμογές υγείας για κινητές συσκευές (εφαρμογές mHealth) για να εξετάσουν το status quo της συμμόρφωσης με τον GDPR στις εφαρμογές Android. Πρώτα προτείνουν ένα αυτοματοποιημένο σύστημα, με το όνομα \mytool, για να γεφυρώσει το σημασιολογικό χάσμα μεταξύ των γενικών κανόνων του GDPR και των εφαρμογών της εφαρμογής, προσδιορίζοντας τις πρακτικές δεδομένων που δηλώνονται στην πολιτική απορρήτου της εφαρμογής και τις σχετικές με τα δεδομένα συμπεριφορές στον κώδικα εφαρμογής. Έπειτα, με βάση το \mytool, εντοπίζουν τρία είδη παραβιάσεων συμμόρφωσης με τον GDPR, συμπεριλαμβανομένης της ελλιπούς πολιτικής απορρήτου, της ασυνέπειας των συλλογών δεδομένων και της ανασφάλειας στη μετάδοση δεδομένων. Πραγματοποιούν μια εμπειρική αξιολόγηση 796 εφαρμογών mHealth. Τα αποτελέσματα αποκαλύπτουν ότι 189 από αυτές δεν παρέχουν πλήρεις πολιτικές απορρήτου. Επιπλέον, 59 εφαρμογές συλλέγουν ευαίσθητα δεδομένα μέσω διαφορετικών μέτρων, αλλά 46 από αυτές περιέχουν τουλάχιστον μία ασυνεπή

συμπεριφορά συλλογής. Ακόμη χειρότερα, μεταξύ των 59 εφαρμογών, μόνο 8 εφαρμογές προσπαθούν να εξασφαλίσουν την ασφάλεια μετάδοσης των συλλεγόμενων δεδομένων. Ωστόσο, οι περισσότερες εφαρμογές περιέχουν τουλάχιστον μία κρυπτογράφηση ή κακή χρήση SSL (Secure Sockets Layer)[1]. Η εργασία τους εκθέτει σοβαρά ζητήματα απορρήτου για να αυξήσει την ευαισθητοποίηση σχετικά με την προστασία του απορρήτου για τους χρήστες και τους προγραμματιστές εφαρμογών, συμπεριλαμβανομένης της μη πληρότητας της πολιτικής απορρήτου, της ασυνέπειας των συλλογών δεδομένων και της ανασφάλειας της μετάδοσης δεδομένων (Fan, και συν., 2020).

Επιπροσθέτως οι Alfawzan, Christen, Spitale, & Biller-Andorno, (2021) πραγματοποίησαν ανασκόπηση εύρους και ανάλυση περιεχομένου των πολιτικών απορρήτου, κοινής χρήσης δεδομένων και ασφάλειας δεδομένων για εφαρμογές mHealth για γυναίκες. Οι εφαρμογές αυτής της κατηγορίας είναι ένα αυξανόμενο φαινόμενο στην παγκόσμια αγορά εφαρμογών για κινητά smartphone. Ένας αυξανόμενος αριθμός γυναικών σε όλο τον κόσμο χρησιμοποιούν εφαρμογές με τη λεγόμενη γυναικεία τεχνολογία (femtech). Δεδομένης της συχνά ιδιωτικής και ευαίσθητης φύσης των δεδομένων που συλλέγονται από τέτοιες εφαρμογές, δικαιολογείται μια ηθική αξιολόγηση από την άποψη του απορρήτου των δεδομένων, της κοινής χρήσης και των πολιτικών ασφάλειας. Ο σκοπός της ανασκόπησης του πεδίου εφαρμογής και της ανάλυσης περιεχομένου είναι να αξιολογήσει την πολιτική απορρήτου, την κοινή χρήση δεδομένων και τις πολιτικές ασφάλειας των εφαρμογών υγείας για γυναίκες για κινητές συσκευές που ισχύουν στη διεθνή αγορά (AppStore's στο σύστημα IOS και GooglePlay's στο σύστημα Android). Εξετάστηκαν 23 πιο δημοφιλείς εφαρμογές mHealth για γυναίκες, εστίασαν σε εφαρμογές που είναι διαθέσιμες στο κοινό τόσο στο Apple AppStore όσο και στο GooglePlay. Οι 23 εφαρμογές που λήφθηκαν αξιολογήθηκαν με μη αυτόματο τρόπο από δύο ανεξάρτητους αναθεωρητές με βάση τον συνδυασμό κριτηρίων απορρήτου και κοινής χρήσης δεδομένων των χρηστών και αξιολόγησης ασφάλειας. Και οι 23 εφαρμογές συνέλεξαν προσωπικά δεδομένα σχετικά με την υγεία. 23 (100%)

[1] Είναι η τυπική τεχνολογία για τη διατήρηση της σύνδεσης στο Διαδίκτυο ασφαλή και την προστασία τυχόν ευαίσθητων δεδομένων που αποστέλλονται μεταξύ δύο συστημάτων, εμποδίζοντας τους εγκληματίες να διαβάσουν και να τροποποιήσουν οποιαδήποτε πληροφορία μεταφέρεται, συμπεριλαμβανομένων πιθανών προσωπικών στοιχείων. Τα δύο συστήματα μπορεί να είναι διακομιστής και πελάτης (για παράδειγμα, ιστότοπος αγορών και πρόγραμμα περιήγησης) ή διακομιστής σε διακομιστή (για παράδειγμα, μια εφαρμογή με προσωπικά αναγνωρίσιμα στοιχεία ή με πληροφορίες μισθοδοσίας).

Αυτό το επιτυγχάνει διασφαλίζοντας ότι τυχόν δεδομένα που μεταφέρονται μεταξύ χρηστών και τοποθεσιών ή μεταξύ δύο συστημάτων παραμένουν αδύνατο να διαβαστούν. Χρησιμοποιεί αλγόριθμους κρυπτογράφησης για την ανακατεύθυνση δεδομένων κατά τη μεταφορά.

επέτρεψαν την παρακολούθηση συμπεριφοράς και 14 (61%) επέτρεψαν την παρακολούθηση τοποθεσίας. Μόνο 16 εφαρμογές (69,5%) εμφάνισαν πολιτική απορρήτου και 12 εφαρμογές (56,5%) ζήτησαν συναίνεση από τους χρήστες, μία εφαρμογή είχε ψευδο-συναίνεση. 3 εφαρμογές συνέλεξαν δεδομένα πριν λάβουν συναίνεση. 20 εφαρμογές (87%) μοιράστηκαν δεδομένα χρηστών με τρίτο μέρος και για τις υπόλοιπες 3 εφαρμογές δεν είναι γνωστό αν μοιράστηκαν δεδομένα ή όχι. Μόνο 13 εφαρμογές (56,5%) παρείχαν πληροφορίες στους χρήστες σχετικά με την ασφάλεια των δεδομένων. Ένα μεγάλο μέρος των πιο δημοφιλών εφαρμογών mHealth για γυναίκες στην αγορά έχουν χαμηλά πρότυπα απορρήτου, κοινής χρήσης και ασφάλειας δεδομένων. Αν και υπάρχουν κανονισμοί, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ (GDPR), οι τρέχουσες πρακτικές των σχετικών εφαρμογών δεν τους ακολουθούν. Τα πρότυπα αποτυχίας των εφαρμογών mHealth για γυναίκες που αξιολογήθηκαν να πληρούν το βασικό απόρρητο και την ασφάλεια των δεδομένων είναι απαράδεκτα τόσο από ηθική όσο και από νομική άποψη (Alfawzan, Christen, Spitale, & Biller-Andorno, 2021).

Στην παρούσα διατριβή θα αναλυθεί ο τρόπος λειτουργίας εφαρμογών που σχετίζονται με την υγεία οι οποίες προωθήθηκαν από κυβερνήσεις χωρών. Με βάση αναφοράς το συναφές θεσμικό πλαίσιο της Ευρωπαϊκής Ένωσης το οποίο θα μελετηθεί, με τη χρήση εργαλείων θα αναλυθούν τα χαρακτηριστικά αυτών των εφαρμογών (ασφάλεια που παρέχουν, διαφάνεια ως προς τη λειτουργία τους, αν επεξεργάζονται μόνο τα απολύτως απαραίτητα δεδομένα και όχι περισσότερα, αν χρησιμοποιούν third party libraries και τι δικαιώματα πρόσβασης λαμβάνουν αυτά τα τρίτα μέλη κτλ.). Ουσιαστικά, θα αποτιμηθεί κατά πόσον οι εφαρμογές που προσφέρονται από δημόσιους φορείς σε αυτόν τον τομέα ακολουθούν τη σχεδιαστική προσέγγιση του «data protection by design» και «data protection by default».

Κεφάλαιο 3
Προστασία προσωπικών δεδομένων

Στο παρόν κεφάλαιο παρουσιάζονται στοιχεία για την Προστασία προσωπικών δεδομένων. Αρχικά αποσαφηνίζονται σχετικές έννοιες, έπειτα καταγράφεται η Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων, ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, η Σύμβαση 108 – Σύμβαση του Συμβουλίου της Ευρώπης και η Εκσυγχρονισμένη Σύμβαση 108, η Κυπριακή Νομοθεσία για τα προσωπικά δεδομένα (πρωταρχικές πράξεις, κανονισμοί, οδηγίες, νομοσχέδια) και τέλος η Ελληνική Νομοθεσία για τα προσωπικά δεδομένα (Ν. 4624/2019, Οδηγία ΕΕ 2016/680, Ν. 2472/1997, Ν. 3471/2006, Συνταγματικά ενοποιημένες Ανεξάρτητες Αρχές).

3.1 Ευρωπαϊκή Νομοθεσία για τα προσωπικά δεδομένα

Το βασικό νομικό κείμενο της ΕΕ σήμερα αναφορικά με την προστασία των προσωπικών δεδομένων ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation – GDPR), ο οποίος είναι σε εφαρμογή από το 2018. Ακολουθούν οι βασικές έννοιες, όπως προσδιορίζονται στον εν λόγω Κανονισμό».

3.1.1 Συνθήκη για την Ευρωπαϊκή Ένωση (άρθρο 6)

Συνθήκη για την Ευρωπαϊκή Ένωση (άρθρο 6) (Consolidated version of the Treaty on European Union, 2012):

1. Η Ένωση αναγνωρίζει τα δικαιώματα, τις ελευθερίες και τις αρχές που ορίζονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης της 7ης Δεκεμβρίου 2000, όπως προσαρμόστηκε στο Στρασβούργο, στις 12 Δεκεμβρίου 2007, ο οποίος έχει την ίδια νομική αξία με τις Συνθήκες. Οι διατάξεις του Χάρτη δεν επεκτείνουν με κανένα τρόπο τις αρμοδιότητες της Ένωσης όπως ορίζονται στις Συνθήκες. Τα δικαιώματα, οι ελευθερίες

και οι αρχές του Χάρτη ερμηνεύονται σύμφωνα με τις γενικές διατάξεις του Τίτλου VII του Χάρτη που διέπουν την ερμηνεία και την εφαρμογή του και λαμβάνοντας δεόντως υπόψη τις επεξηγήσεις που αναφέρονται στον Χάρτη, οι οποίες καθορίζουν τις πηγές αυτών των διατάξεων.

2. Η Ένωση προσχωρεί στην Ευρωπαϊκή Σύμβαση για την Προστασία των Ανθρωπίνων Δικαιωμάτων και των Θεμελιωδών Ελευθεριών. Η προσχώρηση αυτή δεν επηρεάζει τις αρμοδιότητες της Ένωσης όπως ορίζονται στις Συνθήκες.

3. Τα θεμελιώδη δικαιώματα, όπως κατοχυρώνονται από την Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών και όπως απορρέουν από τις κοινές συνταγματικές παραδόσεις των κρατών μελών, αποτελούν γενικές αρχές του δικαίου της Ένωσης.

3.1.2 Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων (Άρθρο 8)

Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων (Άρθρο 8) (European Convention on Human Rights, 2021):

Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής:

1. Καθένας έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας και της αλληλογραφίας του.

2. Δεν επιτρέπεται καμία παρέμβαση δημόσιας αρχής στην άσκηση αυτού του δικαιώματος, εκτός εάν είναι σύμφωνη με τον νόμο και είναι αναγκαία σε μια δημοκρατική κοινωνία προς το συμφέρον της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της οικονομικής ευημερίας της χώρας, για την πρόληψη αταξίας ή εγκληματικότητας, για την προστασία της υγείας ή των ηθών ή για την προστασία των δικαιωμάτων και των ελευθεριών των άλλων.

3.1.3 Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Άρθρο 8)

Προστασία προσωπικών δεδομένων (Official Journal of the European Union, 2012):

1. Καθένας έχει δικαίωμα στην προστασία των προσωπικών δεδομένων που τον αφορούν.

2. Τα δεδομένα αυτά πρέπει να υποβάλλονται σε δίκαιη επεξεργασία για συγκεκριμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερόμενου προσώπου ή κάποια άλλη νόμιμη βάση που ορίζεται από τον νόμο. Καθένας έχει δικαίωμα πρόσβασης σε δεδομένα που έχουν συλλεχθεί που τον αφορούν και δικαίωμα διόρθωσής τους.

3. Η συμμόρφωση με αυτούς τους κανόνες υπόκειται σε έλεγχο από ανεξάρτητη αρχή.

3.1.4 Σύμβαση 108 – Σύμβαση του Συμβουλίου της Ευρώπης

Σύμβαση 108 – Σύμβαση του Συμβουλίου της Ευρώπης για την Προστασία των Ατόμων έναντι της Αυτόματης Επεξεργασίας Προσωπικών Δεδομένων, Στρασβούργο 28/01/1981 (Treaty Office No.108, 1985).

Αυτή η Σύμβαση είναι το πρώτο δεσμευτικό διεθνές μέσο που προστατεύει το άτομο από καταχρήσεις που μπορεί να συνοδεύουν τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα και το οποίο επιδιώκει να ρυθμίσει ταυτόχρονα τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα.

Εκτός από την παροχή εγγυήσεων σε σχέση με τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα, απαγορεύει την επεξεργασία «ευαίσθητων» δεδομένων σχετικά με τη φυλή, την πολιτική, την υγεία, τη θρησκεία, τη σεξουαλική ζωή, το ποινικό μητρώο κ.λπ., ελλείψει κατάλληλων νομικών εγγυήσεων. Η Σύμβαση κατοχυρώνει επίσης το δικαίωμα του ατόμου να γνωρίζει ότι αποθηκεύονται πληροφορίες σε αυτό και, εάν είναι απαραίτητο, να τις διορθώνει.

Ο περιορισμός των δικαιωμάτων που ορίζονται στη Σύμβαση είναι δυνατός μόνο όταν διακυβεύονται υπέρτατα συμφέροντα (π.χ. κρατική ασφάλεια, άμυνα κ.λπ.).

Η Σύμβαση επιβάλλει επίσης ορισμένους περιορισμούς στις διασυνοριακές ροές προσωπικών δεδομένων προς κράτη όπου η νομική ρύθμιση δεν παρέχει ισοδύναμη προστασία.

3.1.5 Εκσυγχρονισμένη Σύμβαση 108

Εκσυγχρονισμένη Σύμβαση 108 – Εκσυγχρονισμένη Σύμβαση του Συμβουλίου της Ευρώπης για την Προστασία των Ατόμων σε σχέση με την Επεξεργασία Προσωπικών Δεδομένων, Δανία, 17-18 Μαΐου 2018 (Ευρωπαϊκή Επιτροπή/COM(2018), 2018):

- Τα κράτη μέλη του Συμβουλίου της Ευρώπης και τα άλλα υπογράφοντα μέρη του παρόντος λαμβάνουν υπόψη ότι ο στόχος του Συμβουλίου της Ευρώπης είναι να επιτύχει μεγαλύτερη ενότητα μεταξύ των μελών του, με βάση ιδίως τον σεβασμό του κράτους δικαίου, καθώς και των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών
- Θεωρώντας ότι είναι απαραίτητο να διασφαλιστεί η ανθρώπινη αξιοπρέπεια και η προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών κάθε ατόμου και, δεδομένης της διαφοροποίησης, εντατικοποίησης και παγκοσμιοποίησης της επεξεργασίας δεδομένων και των ροών προσωπικών δεδομένων, η προσωπική αυτονομία βασίζεται στο δικαίωμα του ατόμου να ελέγχει τα προσωπικά δεδομένα και την επεξεργασία αυτών των δεδομένων
- Υπενθυμίζεται ότι το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα πρέπει να λαμβάνεται υπόψη σε σχέση με τον ρόλο του στην κοινωνία και ότι πρέπει να συμβιβάζεται με άλλα ανθρώπινα δικαιώματα και θεμελιώδεις ελευθερίες, συμπεριλαμβανομένης της ελευθερίας της έκφρασης
- Η παρούσα Σύμβαση επιτρέπει να λαμβάνεται υπόψη, κατά την εφαρμογή των κανόνων που ορίζονται σε αυτήν, η αρχή του δικαιώματος πρόσβασης σε επίσημα έγγραφα

Είναι απαραίτητο, επομένως, να προωθηθούν σε παγκόσμιο επίπεδο οι θεμελιώδεις αξίες του σεβασμού της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων, συμβάλλοντας έτσι στην ελεύθερη ροή πληροφοριών μεταξύ των ανθρώπων (128th Session of the Committee of Ministers, 2018).

3.1.6 Απαίτηση για προστασία δεδομένων από το σχεδιασμό και από προεπιλογή

- **Άρθρο. 25 GDPR: Προστασία δεδομένων από το σχεδιασμό και από προεπιλογή**

1. Λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας, το κόστος εφαρμογής και τη φύση, το εύρος, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους ποικίλης πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που θέτει η επεξεργασία, ο υπεύθυνος επεξεργασίας: τόσο κατά τον καθορισμό των μέσων επεξεργασίας όσο και κατά τη στιγμή της ίδιας της επεξεργασίας, εφαρμόστε κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, τα οποία έχουν σχεδιαστεί για την εφαρμογή αρχών προστασίας

δεδομένων, όπως η ελαχιστοποίηση δεδομένων, με αποτελεσματικό τρόπο. τον τρόπο και την ενσωμάτωση των απαραίτητων διασφαλίσεων στην επεξεργασία προκειμένου να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

2. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας. 2 Η υποχρέωση αυτή ισχύει για τον όγκο των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. 3 Ειδικότερα, τα μέτρα αυτά διασφαλίζουν ότι εξ ορισμού τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του ατόμου σε αόριστο αριθμό φυσικών προσώπων.

3.2 Προσωπικά Δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία που σχετίζεται με αναγνωρισμένο ή αναγνωρίσιμο ζωντανό άτομο. Διαφορετικές πληροφορίες, οι οποίες συλλέγονται μαζί μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης προσωπικά δεδομένα (Ευρωπαϊκή Επιτροπή/Προστασία δεδομένων στην ΕΕ, 2016).

Δεδομένου ότι ο ορισμός περιλαμβάνει «οποιεσδήποτε πληροφορίες», πρέπει να υποθέσει κανείς ότι ο όρος «προσωπικά δεδομένα» πρέπει να ερμηνεύεται όσο το δυνατόν ευρύτερα. Αυτό προτείνεται επίσης στη νομολογία του Ευρωπαϊκού Δικαστηρίου, το οποίο επίσης λαμβάνει υπόψη λιγότερο σαφείς πληροφορίες, όπως καταγραφές ωρών εργασίας που περιλαμβάνουν πληροφορίες σχετικά με την ώρα έναρξης και λήξης της ημέρας εργασίας του εργαζόμενου, καθώς και διαλείμματα ή ώρες δεν εμπίπτουν σε χρόνο εργασίας, ως προσωπικά δεδομένα. Επίσης, οι γραπτές απαντήσεις από έναν υποψήφιο κατά τη διάρκεια μιας δοκιμασίας και τυχόν παρατηρήσεις από τον εξεταστή σχετικά με αυτές τις απαντήσεις αποτελούν «προσωπικά δεδομένα» εάν ο υποψήφιος μπορεί να αναγνωριστεί θεωρητικά. Το ίδιο ισχύει και για τις διευθύνσεις IP. Εάν ο υπεύθυνος επεξεργασίας έχει τη νόμιμη επιλογή να υποχρεώσει τον πάροχο να παραδώσει πρόσθετες πληροφορίες που του επιτρέπουν να αναγνωρίσει τον χρήστη πίσω από τη διεύθυνση IP, και αυτά είναι προσωπικά δεδομένα. Επιπλέον, πρέπει να σημειωθεί ότι τα προσωπικά δεδομένα δεν χρειάζεται να

είναι αντικειμενικά. Υποκειμενικές πληροφορίες όπως απόψεις, κρίσεις ή εκτιμήσεις μπορεί να είναι προσωπικά δεδομένα. Έτσι, αυτό περιλαμβάνει αξιολόγηση της πιστοληπτικής ικανότητας ενός ατόμου ή εκτίμηση της απόδοσης της εργασίας από έναν εργοδότη (GDPR / Personal Data, 2020).

Τέλος, ο νόμος ορίζει ότι οι πληροφορίες για αναφορά προσωπικού πρέπει να αναφέρονται σε φυσικό πρόσωπο. Με άλλα λόγια, η προστασία δεδομένων δεν ισχύει για πληροφορίες σχετικά με νομικά πρόσωπα όπως εταιρείες, ιδρύματα και ιδρύματα. Για τα φυσικά πρόσωπα, από την άλλη, η προστασία αρχίζει και σβήνει με δικαιοπρακτική ικανότητα. Βασικά, ένα άτομο αποκτά αυτή την ικανότητα με τη γέννησή του και τη χάνει με το θάνατό του. Ως εκ τούτου, τα δεδομένα πρέπει να μπορούν να εκχωρηθούν σε αναγνωρισμένα ή αναγνωρίσιμα ζωντανά πρόσωπα για να θεωρηθούν προσωπικά.

Εκτός από τα γενικά δεδομένα προσωπικού χαρακτήρα, πρέπει να ληφθούν υπόψη κυρίως οι ειδικές κατηγορίες προσωπικών δεδομένων (γνωστά και ως ευαίσθητα προσωπικά δεδομένα) που έχουν μεγάλη σημασία επειδή υπόκεινται σε υψηλότερο επίπεδο προστασίας. Αυτά τα δεδομένα περιλαμβάνουν γενετικά, βιομετρικά και δεδομένα υγείας, καθώς και προσωπικά δεδομένα που αποκαλύπτουν φυλετική και εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή ιδεολογικές πεποιθήσεις ή συμμετοχή σε συνδικάτα.

Τα προσωπικά δεδομένα που έχουν αποχαρακτηριστεί, κρυπτογραφηθεί ή ψευδωνυμοποιηθεί, αλλά μπορούν να χρησιμοποιηθούν για τον επαναπροσδιορισμό ενός ατόμου, παραμένουν προσωπικά δεδομένα και εμπίπτουν στο πεδίο εφαρμογής του GDPR.

Επίσης, τα προσωπικά δεδομένα που έχουν καταστεί ανώνυμα με τέτοιο τρόπο ώστε το άτομο να είναι ή να μην είναι πλέον αναγνωρίσιμο δεν θεωρούνται πλέον προσωπικά δεδομένα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμία πρέπει να είναι μη αναστρέψιμη.

Ο GDPR προστατεύει τα προσωπικά δεδομένα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία αυτών των δεδομένων – είναι τεχνολογικά ουδέτερος και ισχύει τόσο για την αυτοματοποιημένη όσο και για τη μη αυτόματη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα είναι οργανωμένα σύμφωνα με προκαθορισμένα κριτήρια (για παράδειγμα αλφαβητική σειρά). Επίσης, δεν έχει σημασία πώς αποθηκεύονται τα δεδομένα – σε ένα σύστημα πληροφορικής, μέσω

βιντεοεπιτήρησης ή σε χαρτί. Σε όλες τις περιπτώσεις, τα προσωπικά δεδομένα υπόκεινται στις απαιτήσεις προστασίας που ορίζονται στον GDPR (Ευρωπαϊκή Επιτροπή/Προστασία δεδομένων στην ΕΕ, 2016).

Παραδείγματα προσωπικών δεδομένων είναι τα:

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- διεύθυνση email όπως name.surname@gmail.com
- αριθμός ταυτότητας
- δεδομένα τοποθεσίας (για παράδειγμα η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση Πρωτοκόλλου Διαδικτύου (Internet Protocol / IP)
- αναγνωριστικό cookie
- αναγνωριστικό διαφήμισης του τηλεφώνου
- δεδομένα που διατηρούνται από ένα νοσοκομείο ή έναν γιατρό, τα οποία προσδιορίζουν μοναδικά ένα άτομο.

Παραδείγματα δεδομένων που δεν θεωρούνται προσωπικά δεδομένα είναι τα:

- αριθμός μητρώου εταιρείας
- διεύθυνση email όπως info@company.com
- ανώνυμα δεδομένα

3.2.1 Απαίτηση για διαφάνεια της επεξεργασίας

- **Άρθρο. 13 GDPR: Πληροφορίες που πρέπει να παρέχονται όταν συλλέγονται προσωπικά δεδομένα από το υποκείμενο των δεδομένων**

1. Όταν δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ένα υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, τη στιγμή που λαμβάνονται τα προσωπικά δεδομένα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες (IntersoftGeneral/Άρθρο 13: GDPR, 2016):

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας·

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση·

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα προσωπικά δεδομένα καθώς και τη νομική βάση για την επεξεργασία·

δ) όταν η επεξεργασία βασίζεται στο στοιχείο του άρθρου 6 παράγραφος 1, τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος·

ε) τους παραλήπτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν·

στ) κατά περίπτωση, το γεγονός ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή απουσία απόφασης επάρκειας από την Επιτροπή, ή στην περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 46 ή 47 ή στο δεύτερο εδάφιο του άρθρου 49 παράγραφος 1, αναφορά στις κατάλληλες ή κατάλληλες διασφαλίσεις και στα μέσα για τη λήψη αντιγράφου αυτών ή όταν έχουν διατεθεί.

2. Εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες περαιτέρω πληροφορίες που είναι απαραίτητες για τη διασφάλιση της δίκαιης και διαφανούς επεξεργασίας, τη στιγμή που λαμβάνονται τα δεδομένα προσωπικού χαρακτήρα:

α) την περίοδο για την οποία θα αποθηκευτούν τα προσωπικά δεδομένα ή, εάν αυτό δεν είναι δυνατό, τα κριτήρια που χρησιμοποιούνται για τον καθορισμό αυτής της περιόδου·

β) την ύπαρξη του δικαιώματος να ζητήσει από τον υπεύθυνο επεξεργασίας πρόσβαση και διόρθωση ή διαγραφή προσωπικών δεδομένων ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων ή αντίρρηση στην επεξεργασία καθώς και το δικαίωμα στη φορητότητα των δεδομένων·

γ) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο β), η ύπαρξη του δικαιώματος ανάκλησης της

συγκατάθεσης ανά πάσα στιγμή, χωρίς να επηρεάζεται η νομιμότητα της επεξεργασίας με βάση τη συγκατάθεση πριν από την απόσυρσή του·

δ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή·

ε) εάν η παροχή προσωπικών δεδομένων αποτελεί νομική ή συμβατική απαίτηση ή απαίτηση απαραίτητη για τη σύναψη σύμβασης, καθώς και εάν το υποκείμενο των δεδομένων υποχρεούται να παράσχει τα προσωπικά δεδομένα και τις πιθανές συνέπειες της μη παροχής αυτών των δεδομένων·

στ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον σε αυτές τις περιπτώσεις, ουσιαστικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων.

3. Όταν ο υπεύθυνος επεξεργασίας σκοπεύει να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για σκοπό διαφορετικό από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για αυτόν τον άλλο σκοπό και κάθε σχετική περαιτέρω πληροφορία όπως αναφέρεται στην παράγραφο 2.

4. Οι παράγραφοι 1, 2 και 3 δεν εφαρμόζονται όταν και εφόσον το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες.

- **Άρθρο. 14 GDPR Πληροφορίες που πρέπει να παρέχονται όταν τα προσωπικά δεδομένα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων**

1. Σε περίπτωση που δεν έχουν ληφθεί προσωπικά δεδομένα από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες (Intersoft consulting/Άρθρο 14 GDPR, 2016):

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας·

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση·

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα προσωπικά δεδομένα καθώς και τη νομική βάση για την επεξεργασία·

δ) τις σχετικές κατηγορίες προσωπικών δεδομένων·

ε) τους παραλήπτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν·

στ) κατά περίπτωση, ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε παραλήπτη σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή απουσία απόφασης επάρκειας από την Επιτροπή, ή στην περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 46 ή 47 , ή δεύτερο εδάφιο του άρθρου 49 παράγραφος 1, αναφορά στις κατάλληλες ή κατάλληλες διασφαλίσεις και στα μέσα για τη λήψη αντιγράφου αυτών ή όταν έχουν διατεθεί.

2. Εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 1, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες που είναι απαραίτητες για τη διασφάλιση δίκαιης και διαφανούς επεξεργασίας σε σχέση με το υποκείμενο των δεδομένων:

α) την περίοδο για την οποία θα αποθηκευτούν τα προσωπικά δεδομένα ή, εάν αυτό δεν είναι δυνατό, τα κριτήρια που χρησιμοποιούνται για τον καθορισμό αυτής της περιόδου·

β) όταν η επεξεργασία βασίζεται στο στοιχείο στ) του άρθρου 6 παράγραφος 1, τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος·

γ) την ύπαρξη του δικαιώματος να ζητήσει από τον υπεύθυνο επεξεργασίας πρόσβαση και διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων και αντίρρηση στην επεξεργασία καθώς και το δικαίωμα στη φορητότητα των δεδομένων·

δ) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α) , η ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης ανά πάσα στιγμή, χωρίς να επηρεάζεται η νομιμότητα της επεξεργασίας που βασίζεται στη συγκατάθεση πριν από αυτήν απόσυρση;

ε) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή·

στ) από ποια πηγή προέρχονται τα προσωπικά δεδομένα και, εάν ισχύει, εάν προέρχονται από πηγές προσβάσιμες στο κοινό·

ζ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον σε αυτές τις περιπτώσεις, ουσιαστικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων.

3. Ο υπεύθυνος επεξεργασίας παρέχει τις πληροφορίες που αναφέρονται στις παραγράφους 1 και 2:

α) εντός εύλογου χρονικού διαστήματος από τη λήψη των προσωπικών δεδομένων, αλλά το αργότερο εντός ενός μηνός, λαμβανομένων υπόψη των ειδικών συνθηκών υπό τις οποίες υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα·

β) εάν τα προσωπικά δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο των δεδομένων, το αργότερο κατά τη στιγμή της πρώτης επικοινωνίας με αυτό το υποκείμενο των δεδομένων· ή

γ) εάν προβλέπεται γνωστοποίηση σε άλλον παραλήπτη, το αργότερο κατά την πρώτη αποκάλυψη των προσωπικών δεδομένων.

4. Όταν ο υπεύθυνος επεξεργασίας σκοπεύει να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για άλλο σκοπό από αυτόν για τον οποίο ελήφθησαν τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για αυτόν τον άλλο σκοπό και κάθε σχετική περαιτέρω πληροφορία όπως αναφέρεται στην παράγραφο 2.

5. Οι παράγραφοι 1 έως 4 δεν εφαρμόζονται όταν και εφόσον:

α) το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες·

β) η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια, ιδίως για την επεξεργασία για σκοπούς αρχειοθέτησης προς δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή

στατιστικούς σκοπούς, υπό τους όρους και τις διασφαλίσεις που αναφέρονται στο άρθρο 89 παράγραφος 1 ή στο βαθμό που η υποχρέωση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου είναι πιθανό να καταστήσει αδύνατη ή να βλάψει σοβαρά την επίτευξη των στόχων αυτής της επεξεργασίας. Σε τέτοιες περιπτώσεις, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, συμπεριλαμβανομένης της δημοσιοποίησης των πληροφοριών·

γ) η απόκτηση ή η αποκάλυψη ορίζεται ρητά από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο παρέχει τα κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων· ή

δ) όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά με την επιφύλαξη υποχρέωσης επαγγελματικού απορρήτου που ρυθμίζεται από το δίκαιο της Ένωσης ή του κράτους μέλους, συμπεριλαμβανομένης της νομικής υποχρέωσης εχεμύθειας.

3.3 Κυπριακή Νομοθεσία για τα προσωπικά δεδομένα

Η προστασία δεδομένων στην Κύπρο διέπεται κυρίως από τον Γενικό Κανονισμό για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) («GDPR» / General Data Protection Regulation) ο οποίος έχει ενσωματωθεί στο κυπριακό δίκαιο δυνάμει του Νόμου 125(I) του 2018 που προβλέπει την προστασία των φυσικών Πρόσωπα αλληλένδετα με την Επεξεργασία Προσωπικών Δεδομένων και για την Ελεύθερη Διακίνηση Τέτοιων Δεδομένων («ο Νόμος»).

Στη συνέχεια παρατίθενται οι νόμοι της κυπριακής νομοθεσίας όσον αφορά τα προσωπικά δεδομένα (Νεοκλέους, 2022), (Republic of Cyprus/Law 125(I)2018, 2018):

3.3.1 Πρωταρχικές πράξεις, κανονισμοί, οδηγίες, νομοσχέδια

Ο Νόμος που τέθηκε σε ισχύ, στις 31 Ιουλίου 2018, εφάρμοσε ορισμένες διατάξεις του GDPR και κατήργησε τον περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία Προσώπων) Νόμο 138 (I) 2001, ο οποίος είχε εφαρμόσει την Οδηγία για την Προστασία Δεδομένων (Οδηγία 95/46/ΕΚ)).

3.3.2 Κατευθυντήριες γραμμές

Για να διασφαλιστεί η ορθή εφαρμογή του GDPR, το Γραφείο του Επιτρόπου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα («ο Επίτροπος») έχει υιοθετήσει ορισμένες κατευθυντήριες γραμμές που εκδόθηκαν από την ομάδα εργασίας του άρθρου 29 («WP29»), η οποία έχει αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («EDPB») και έχει επίσης εκδώσει τις δικές του κατευθυντήριες γραμμές και γνώμες.

Οι κατευθυντήριες γραμμές του Επιτρόπου καλύπτουν ειδικότερα:

- Υπεύθυνοι προστασίας δεδομένων («Καθοδήγηση DPO»)
- Εκτιμήσεις επιπτώσεων στην προστασία δεδομένων («Καθοδήγηση DPIA»)
- Ειδοποιήσεις παραβίασης προσωπικών δεδομένων
- Κώδικες δεοντολογίας και μηχανισμοί πιστοποίησης
- Ασφάλεια επεξεργασίας και τις οδηγίες για την ασφάλεια της επεξεργασίας
- Μεταφορές δεδομένων
- Οδηγός για τα αρχεία των δραστηριοτήτων επεξεργασίας και Οδηγός για τη συμπλήρωση του αρχείου των δραστηριοτήτων επεξεργασίας .
- Βιντεοπαρακολούθηση
- Εργασιακές σχέσεις
- Χρήση του διαδικτύου και των κινητών τηλεφώνων
- Άμεσο μάρκετινγκ αγαθών και υπηρεσιών
- Οδηγίες προς τραπεζικά ιδρύματα σχετικά με τις περιόδους διατήρησης προσωπικών δεδομένων
- Οδηγίες για πολιτικές επικοινωνίες μέσω τηλεφωνημάτων
- Μετάδοση μηνυμάτων και πραγματοποίηση κλήσεων με πολιτικό περιεχόμενο/προώθηση υποψηφίων

- Οδηγίες για την άσκηση του δικαιώματος πρόσβασης των δημοσίων υπαλλήλων
- Οδηγίες σχετικά με τις περιόδους διατήρησης ιατρικών δεδομένων
- Γνώμη 1/2018 που απευθύνεται σε Συνδικαλιστικές Οργανώσεις σχετικά με την κοινοποίηση από τους εργοδότες καταλόγων με ονόματα εργαζομένων, τους μισθούς και τις εισφορές τους
- Γνώμη 2/2018 σχετικά με τη βιντεοπαρακολούθηση στην εργασία και τη χρήση βιομετρικών συστημάτων
- Γνώμη 1/2019 σχετικά με την πρόσβαση σε λογαριασμούς email υπαλλήλου και πρώην υπαλλήλου
- Ερμηνεία του άρθρου 10 του ΓΚΠΔ.
- Γνώμη 1/2020 σχετικά με την επίβλεψη υπεραστικών/ διαδικτυακών εξετάσεων από ιδρύματα τριτοβάθμιας εκπαίδευσης (διαθέσιμη μόνο στα ελληνικά εδώ) . και
- Οδηγία 4/2017 για δικαίωμα πρόσβασης εργαζομένων ή υποψηφίων στο Δημόσιο Τμήμα.

Πέραν των ανωτέρω κατευθυντήριων γραμμών, ο Επίτροπος έχει εκδώσει και οδηγίες με τη μορφή δημόσιων ανακοινώσεων, ως εξής:

- ❖ συναίνεση στο πλαίσιο του άμεσου μάρκετινγκ (SMS και email)
- ❖ ανακοίνωση σχετικά με τις υφιστάμενες άδειες μεταφοράς· και
- ❖ δείγμα καταγραφής δραστηριοτήτων επεξεργασίας και οδηγίες ολοκλήρωσής της.

Επιπλέον, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («EDPB») δημοσίευσε την ακόλουθη Γνώμη για την Κύπρο:

- ❖ Γνώμη 10/2019 σχετικά με το σχέδιο καταλόγου της αρμόδιας εποπτικής αρχής της Κύπρου σχετικά με τις εργασίες επεξεργασίας που υπόκεινται στην απαίτηση εκτίμησης επιπτώσεων στην προστασία δεδομένων (άρθρο 35 παράγραφος 4 GDPR)

3.3.3 Νομολογία

Από την έναρξη ισχύος του GDPR στην Κύπρο, έχουν διερευνηθεί από τον Επίτροπο μια σειρά υποθέσεων κατά ιδιωτικών οργανισμών και δημόσιων αρχών, για τις οποίες έχουν εκδοθεί δημόσιες ανακοινώσεις.

Οι περιλήψεις των αποφάσεων του Επιτρόπου είναι διαθέσιμες σε εκθέσεις που δημοσιεύονται καθ' όλη τη διάρκεια του έτους.

3.3.4 Πεδίο εφαρμογής

Δεν υπάρχουν εθνικές αποκλίσεις από τον GDPR για τα εξής:

- Προσωπικό πεδίο εφαρμογής
- Εδαφική εμβέλεια
- Πεδίο εφαρμογής υλικού

3.4 Ελληνική Νομοθεσία για τα προσωπικά δεδομένα

Στη συνέχεια παρατίθενται οι νόμοι της ελληνικής νομοθεσίας όσον αφορά τα προσωπικά δεδομένα:

- Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) (2016/679) (GDPR)
- Προστασία φυσικών προσώπων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ.
- Ν. 4624/2019: Είναι ο νόμος ο οποίος, μεταξύ άλλων, υλοποιεί στην ελληνική νομοθεσία κάποια ζητήματα για τα οποία ο GDPR αφήνει διακριτική ευχέρεια στον εθνικό νομοθέτη. Με το νόμο αυτό ως αρμόδια ανεξάρτητη εποπτική Αρχή για τον έλεγχο της εφαρμογής της σχετικής νομοθεσίας στην Ελλάδα ορίζεται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).
- Ν. 3471/2006: Ο νόμος 3471/2006 ενσωματώνει στο ελληνικό εθνικό δίκαιο την Οδηγία 2002/58/ΕΚ (e-Privacy Οδηγία) μετά την τροποποίησή της από την Οδηγία 2009/136/ΕΚ. Η εν λόγω Οδηγία έχει επίσης εφαρμογή σε περιπτώσεις «έξυπνων» εφαρμογών, για περιπτώσεις όπως, π.χ., η χρήση cookies.

3.5 Συμπερασματικά

Συμπερασματικά, και με απλά λόγια, η νομοθεσία για τα προσωπικά δεδομένα στην Ευρώπη δίνει μεταξύ άλλων έμφαση στη διαφάνεια της επεξεργασίας, στο ότι πρέπει να συλλέγονται τα απολύτως απαραίτητα δεδομένα και όχι περισσότερα από ό,τι απαιτείται: αυτό θα πρέπει να γίνεται εξ αρχής, ενώ οι προκαθορισμένες ρυθμίσεις μίας εφαρμογής θα πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα.

Αν και ο GDPR είναι ευρωπαϊκός κανονισμός, εν τούτοις έχει εφαρμογή σε οποιονδήποτε οργανισμό παρέχει υπηρεσίες σε πολίτες της ΕΕ.

Κεφάλαιο 4
Εφαρμογές Android και Προστασία προσωπικών δεδομένων

Στο 4ο κεφάλαιο για τις εφαρμογές Android και την προστασία προσωπικών δεδομένων καταγράφονται στοιχεία για το λειτουργικό Android, τα χαρακτηριστικά του (διεπαφή, αρχική οθόνη, γραμμή κατάστασης, ειδοποιήσεις, λίστες εφαρμογών, κουμπιά πλοήγησης, προβολή διαιρεμένης οθόνης, φόρτιση κατά την απενεργοποίηση), και τέλος η ασφάλεια και ιδιωτικότητα (τεχνικά χαρακτηριστικά ασφαλείας, συνήθεις απειλές για την ασφάλεια, εντοπισμός τοποθεσίας, περαιτέρω δικλείδες ασφαλείας).

4.1 Λειτουργικό Android

Το Android είναι ένα λειτουργικό σύστημα για κινητές τερματικές συσκευές που βασίζεται σε μια τροποποιημένη έκδοση του πυρήνα Linux και άλλου λογισμικού ανοιχτού κώδικα, σχεδιασμένο κυρίως για κινητές συσκευές με οθόνη αφής, όπως το smartphone και το tablet. Το Android αναπτύσσεται από μια κοινοπραξία προγραμματιστών γνωστή ως Open Handset Alliance[2], αν και η πιο ευρέως χρησιμοποιούμενη έκδοσή του αναπτύσσεται κυρίως από την Google. Αποκαλύφθηκε τον Νοέμβριο του 2007, με την πρώτη εμπορική συσκευή Android, το HTC Dream, και λανσαρίστηκε τον Σεπτέμβριο του 2008 (Britannica/Android operating system, 2022).

[2] Είναι μια κοινοπραξία 84 εταιρειών για την ανάπτυξη ανοιχτών προτύπων για κινητές συσκευές. Οι εταιρείες-μέλη περιλαμβάνουν τις HTC, Sony, Dell, Intel, Motorola, Qualcomm, Texas Instruments, Google, Samsung Electronics, LG Electronics, T-Mobile, Sprint Corporation, Nvidia και Wind River Systems.

Στον πυρήνα του, το λειτουργικό σύστημα είναι γνωστό ως Android Open Source Project (AOSP) και είναι ελεύθερο λογισμικό ανοιχτού κώδικα (free and open-source software / FOSS) με άδεια κατά κύριο λόγο με την άδεια Apache. Ωστόσο, οι περισσότερες συσκευές λειτουργούν στην ιδιόκτητη έκδοση Android που αναπτύχθηκε από την Google, η οποία διατίθεται με προεγκατεστημένο πρόσθετο ιδιόκτητο λογισμικό κλειστού κώδικα, κυρίως το Google Mobile Services (GMS) που περιλαμβάνει βασικές εφαρμογές όπως το Google Chrome, την πλατφόρμα ψηφιακής διανομής Google Play και τις σχετικές Υπηρεσίες Google Play πλατφόρμα ανάπτυξης. Ενώ το AOSP είναι δωρεάν, το όνομα και το λογότυπο «Android» είναι εμπορικά σήματα της Google, η οποία επιβάλλει πρότυπα για τον περιορισμό της χρήσης της επωνυμίας Android από «μη πιστοποιημένες» συσκευές εκτός του οικοσυστήματος τους (Callaham, 2022).

Πάνω από το 70 % των smartphone που βασίζονται στο Android Open Source Project εκτελούν το οικοσύστημα της Google (το οποίο είναι γνωστό ως απλά Android), ορισμένα με διεπαφές χρήστη και σουίτες λογισμικού προσαρμοσμένες από τον προμηθευτή, όπως το TouchWiz και αργότερα το One UI από τη Samsung και το HTC Sense. Τα ανταγωνιστικά οικοσυστήματα και τα forks του AOSP περιλαμβάνουν το Fire OS (αναπτύχθηκε από την Amazon), το ColorOS από την OPPO, το OriginOS από τη Vivo, το MagicUI από την Honor ή προσαρμοσμένες ROM όπως το LineageOS (Guerra-Manzanares, Luckner, & Bahsi, 2022).

Ο πηγαίος κώδικας έχει χρησιμοποιηθεί για την ανάπτυξη παραλλαγών του Android σε μια σειρά άλλων ηλεκτρονικών ειδών, όπως κονσόλες παιχνιδιών, ψηφιακές φωτογραφικές μηχανές, φορητές συσκευές αναπαραγωγής πολυμέσων και υπολογιστές, το καθένα με μια εξειδικευμένη διεπαφή χρήστη. Ορισμένα γνωστά παράγωγα περιλαμβάνουν το Android TV για τηλεοράσεις και το Wear OS για φορητές συσκευές, που αναπτύχθηκαν και τα δύο από την Google. Τα πακέτα λογισμικού στο Android, τα οποία χρησιμοποιούν τη μορφή APK[3], διανέμονται γενικά μέσω ιδιόκτητων καταστημάτων εφαρμογών όπως το Google Play Store, το Amazon Appstore (συμπεριλαμβανομένων των Windows 11), το Samsung Galaxy Store, το Huawei

[3] Το Πακέτο Android με την επέκταση αρχείου apk είναι η μορφή αρχείου που χρησιμοποιείται από το λειτουργικό σύστημα Android και από μια σειρά άλλα λειτουργικά συστήματα που βασίζονται σε Android για διανομή και εγκατάσταση εφαρμογών για κινητά, παιχνίδια για κινητά και ενδιάμεσο λογισμικό.

AppGallery, το Cafe Bazaar και το GetJar ή πλατφόρμες ανοιχτού κώδικα όπως το Aptoide ή το F-Droid (Mazuera-Rozo, και συν., 2022).

Το Android είναι το λειτουργικό σύστημα με τις περισσότερες πωλήσεις παγκοσμίως σε smartphone από το 2011 και σε tablet από το 2013. Από τον Μάιο του 2021, είχε πάνω από τρία δισεκατομμύρια μηνιαίους ενεργούς χρήστες, τη μεγαλύτερη εγκατεστημένη βάση οποιουδήποτε λειτουργικού συστήματος, και από τον Ιανουάριο του 2021, το Google Play Store παρουσίαζε πάνω από 3 εκατομμύρια εφαρμογές. Το Android 13, που κυκλοφόρησε στις 15 Αυγούστου 2022, είναι η πιο πρόσφατη έκδοση κατά τη στιγμή που γράφονται οι γραμμές αυτές, και το Android 12.1/12L που κυκλοφόρησε πρόσφατα περιλαμβάνει βελτιώσεις ειδικά για πτυσσόμενα τηλέφωνα, tablet, οθόνες μεγέθους επιφάνειας εργασίας και Chromebook (Bhatt & Furia, 2022).

4.2 Χαρακτηριστικά του Android

Στην παρούσα υποενότητα θα παρουσιαστούν διάφορα χαρακτηριστικά του Android όπως: η Διεπαφή, η Αρχική οθόνη, η Γραμμή κατάστασης, οι Ειδοποιήσεις, οι Λίστες εφαρμογών, τα Κουμπιά πλοήγησης, η Προβολή διαιρεμένης οθόνης,

4.2.1 Διεπαφή

Η προεπιλεγμένη διεπαφή χρήστη του Android βασίζεται κυρίως σε άμεσο χειρισμό, χρησιμοποιώντας εισόδους αφής που αντιστοιχούν σε πραγματικές ενέργειες, όπως σάρωση, πάτημα / tapping, pinching, για χειρισμό αντικειμένων στην οθόνη, μαζί με εικονικό πληκτρολόγιο. Οι ελεγκτές παιχνιδιών και τα φυσικά πληκτρολόγια πλήρους μεγέθους υποστηρίζονται μέσω Bluetooth ή USB. Η απόκριση στην είσοδο του χρήστη έχει σχεδιαστεί για να είναι άμεση και παρέχει μια διεπαφή αφής, χρησιμοποιώντας συχνά τις δυνατότητες δόνησης της συσκευής για την παροχή απτικής ανάδρασης στον χρήστη. Εσωτερικό υλικό, όπως επιταχυνσιόμετρα, γυροσκόπια και αισθητήρες εγγύτητας χρησιμοποιούνται από ορισμένες εφαρμογές για να ανταποκρίνονται σε πρόσθετες ενέργειες του χρήστη, για παράδειγμα προσαρμόζοντας την οθόνη από κατακόρυφο σε οριζόντιο προσανατολισμό ανάλογα με τον προσανατολισμό της συσκευής, ή επιτρέποντας στον χρήστη να κατευθύνει ένα όχημα σε ένα παιχνίδι αγώνων περιστρέφοντας τη συσκευή, κάνοντας προσομοίωση ελέγχου ενός τιμονιού (Elprocus/Android Operating System & Its Features, 2022), (Tang, Li, Jiang, Gu, & Li, 2022).

4.2.2 Αρχική οθόνη

Οι συσκευές Android εκκινούνται στην αρχική οθόνη, τον κύριο «κόμβο» πλοήγησης και πληροφοριών σε συσκευές Android, ανάλογο με τον επιτραπέζιο υπολογιστή που βρίσκεται σε προσωπικούς υπολογιστές. Οι αρχικές οθόνες Android αποτελούνται συνήθως από εικονίδια εφαρμογών και γραφικά στοιχεία. Τα εικονίδια εφαρμογών εκκινούν τη συσχετισμένη εφαρμογή, ενώ τα γραφικά στοιχεία εμφανίζουν ζωντανά περιεχόμενο που ενημερώνεται αυτόματα, όπως πρόγνωση καιρού, τα εισερχόμενα email του χρήστη ή ένα ticker ειδήσεων απευθείας στην αρχική οθόνη. Μια αρχική οθόνη μπορεί να αποτελείται από πολλές σελίδες, μεταξύ των οποίων ο χρήστης μπορεί να κάνει σάρωση εμπρός και πίσω. Οι εφαρμογές τρίτων που είναι διαθέσιμες στο Google Play και σε άλλα καταστήματα εφαρμογών μπορούν να εμφανίζονται εκτενώς στην αρχική οθόνη, και ακόμη και να μιμηθούν την εμφάνιση άλλων λειτουργικών συστημάτων, όπως το Windows Phone. Οι περισσότεροι κατασκευαστές προσαρμόζουν την εμφάνιση και τις δυνατότητες των συσκευών τους Android για να διαφοροποιηθούν από τους ανταγωνιστές τους (Elprocus/Android Operating System & Its Features, 2022).

4.2.3 Γραμμή κατάστασης

Στο επάνω μέρος της οθόνης υπάρχει μια γραμμή κατάστασης, η οποία εμφανίζει πληροφορίες σχετικά με τη συσκευή και τη σύνδεσή της. Αυτή η γραμμή κατάστασης μπορεί να «τραβηχτεί» (σύρεται) προς τα κάτω για να αποκαλυφθεί μια οθόνη ειδοποιήσεων όπου οι εφαρμογές εμφανίζουν σημαντικές πληροφορίες ή ενημερώσεις, καθώς και γρήγορη πρόσβαση σε στοιχεία ελέγχου συστήματος και εναλλαγές όπως φωτεινότητα οθόνης, ρυθμίσεις συνδεσιμότητας (WiFi, Bluetooth, δεδομένα κινητής τηλεφωνίας), λειτουργία ήχου και φακός. Οι προμηθευτές μπορούν να εφαρμόσουν εκτεταμένες ρυθμίσεις, όπως η δυνατότητα προσαρμογής της φωτεινότητας του φακού (Tang, Li, Jiang, Gu, & Li, 2022).

4.2.4 Ειδοποιήσεις

Οι ειδοποιήσεις είναι «σύντομες, έγκαιρες και σχετικές πληροφορίες σχετικά με την εφαρμογή όταν δεν χρησιμοποιείται» και όταν πατηθούν, οι χρήστες οδηγούνται σε μια οθόνη εντός της εφαρμογής που σχετίζεται με την ειδοποίηση. Ξεκινώντας με το Android 4.1 «Jelly Bean», οι «επεκτάσιμες ειδοποιήσεις» επιτρέπουν στον χρήστη να πατήσει ένα εικονίδιο στην ειδοποίηση για να επεκτείνει και να εμφανίσει περισσότερες πληροφορίες

και πιθανές ενέργειες εφαρμογής απευθείας από την ειδοποίηση (Tang, Li, Jiang, Gu, & Li, 2022).

4.2.5 Λίστες εφαρμογών

Η επιλογή «Όλες οι εφαρμογές» εμφανίζει όλες τις εγκατεστημένες εφαρμογές, με τη δυνατότητα για τους χρήστες να σύρουν μια εφαρμογή από τη λίστα στην αρχική οθόνη. Η πρόσβαση στη λίστα εφαρμογών μπορεί να γίνει χρησιμοποιώντας μια κίνηση ή ένα κουμπί, ανάλογα με την έκδοση Android. Η οθόνη «Πρόσφατα», γνωστή και ως «Επισκόπηση», επιτρέπει στους χρήστες να αλλάζουν μεταξύ εφαρμογών που χρησιμοποιήθηκαν πρόσφατα. Η πρόσφατη λίστα μπορεί να εμφανίζεται δίπλα-δίπλα ή να επικαλύπτεται, ανάλογα με την έκδοση Android και τον κατασκευαστή (Perkins, 2023).

4.2.6 Κουμπιά πλοήγησης

Πολλά πρώιμα smartphone με λειτουργικό Android ήταν εξοπλισμένα με ένα αποκλειστικό κουμπί αναζήτησης για γρήγορη πρόσβαση σε μια μηχανή αναζήτησης ιστού και στη λειτουργία εσωτερικής αναζήτησης μεμονωμένων εφαρμογών. Οι πιο πρόσφατες συσκευές συνήθως επιτρέπουν την πρώτη με παρατεταμένο πάτημα ή σάρωση μακριά από το κουμπί αρχικής οθόνης (Perkins, 2023).

Το αποκλειστικό κλειδί επιλογής, γνωστό και ως πλήκτρο «μενού», και η προσομοίωσή του στην οθόνη, δεν υποστηρίζεται πλέον από την έκδοση Android 10. Η Google συνιστά στους προγραμματιστές εφαρμογών για κινητά να εντοπίζουν τα μενού μέσα στη διεπαφή χρήστη. Σε πιο πρόσφατα τηλέφωνα, η θέση του καταλαμβάνεται από ένα πλήκτρο εργασίας που χρησιμοποιείται για πρόσβαση στη λίστα των πρόσφατα χρησιμοποιημένων εφαρμογών όταν ενεργοποιείται. Ανάλογα με τη συσκευή, το παρατεταμένο πάτημά της μπορεί να προσομοιώνει ένα πάτημα κουμπιού μενού ή να ενεργοποιεί την προβολή διαχωρισμένης οθόνης, η τελευταία από τις οποίες είναι η προεπιλεγμένη συμπεριφορά από την έκδοση 7 του stock Android (Perkins, 2023).

4.2.7 Προβολή διαιρεμένης οθόνης

Η εγγενής υποστήριξη για προβολή διαίρεσης οθόνης έχει προστεθεί στην έκδοση Android 7.0 Nougat. Τα πρώτα προσαρμοσμένα από προμηθευτές smartphone που βασίζονται σε Android που είναι γνωστό ότι διέθεταν λειτουργία προβολής διαχωρισμένης οθόνης είναι τα Samsung Galaxy S3 και Note 2 του 2012, το πρώτο από

τα οποία έλαβε αυτήν τη δυνατότητα με την αναβάθμιση premium σουίτας που παρέχεται στο TouchWiz με Android 4.1 Jelly Bean (Perkins, 2023).

4.2.8 Φόρτιση κατά την απενεργοποίηση

Όταν συνδέεται ή αποσυνδέεται η τροφοδοσία φόρτισης και όταν ενεργοποιείται το κουμπί λειτουργίας ή το κουμπί αρχικής οθόνης, ενώ η συσκευή είναι απενεργοποιημένη, εμφανίζεται στην οθόνη ένας οπτικός μετρητής μπαταρίας του οποίου η εμφάνιση ποικίλλει μεταξύ των προμηθευτών, επιτρέποντας στον χρήστη να εκτιμήσει γρήγορα την κατάσταση φόρτισης χωρίς να χρειάζεται να γίνει εκκίνηση πρώτα. Ορισμένα, μάλιστα, εμφανίζουν και το ποσοστό της μπαταρίας (Perkins, 2023).

4.3 Εφαρμογές του Android

Πολλές, σχεδόν όλες, συσκευές Android διαθέτουν προεγκατεστημένες εφαρμογές Google, όπως το Gmail, οι Χάρτες Google, το Google Chrome, το YouTube, η Μουσική Google Play, οι Ταινίες & TV Google Play και πολλά άλλα.

Οι εφαρμογές, που επεκτείνουν τη λειτουργικότητα των συσκευών (και πρέπει να είναι 64-bit), έχουν γραφτεί χρησιμοποιώντας το κιτ ανάπτυξης λογισμικού Android (software development kit / SDK) και, συχνά, τη γλώσσα προγραμματισμού Kotlin, η οποία αντικατέστησε την Java ως η προτιμώμενη γλώσσα της Google για την ανάπτυξη εφαρμογών Android τον Μάιο του 2019, ενώ είχε ανακοινωθεί αρχικά τον Μάιο του 2017. Η Java εξακολουθεί να υποστηρίζεται (αρχικά η μόνη επιλογή για προγράμματα χώρου χρήστη και συχνά αναμιγνύεται με την Kotlin), όπως είναι η C++. Η Java ή άλλες γλώσσες JVM, όπως η Kotlin, μπορούν να συνδυαστούν με C /C++, μαζί με μια επιλογή από μη προεπιλεγμένους χρόνους εκτέλεσης που επιτρέπουν καλύτερη υποστήριξη C++. Η γλώσσα προγραμματισμού Go υποστηρίζεται επίσης, αν και με περιορισμένο σύνολο διεπαφών προγραμματισμού εφαρμογών (application programming interfaces / API) (Amer & El-Sappagh, 2022).

Το SDK περιλαμβάνει ένα ολοκληρωμένο σύνολο εργαλείων ανάπτυξης, που περιλαμβάνει ένα πρόγραμμα εντοπισμού σφαλμάτων, βιβλιοθήκες λογισμικού, έναν εξομοιωτή συσκευής που βασίζεται σε QEMU[4], τεκμηρίωση, και δείγμα κώδικα. Αρχικά,

[4] Το QEMU είναι ένας δωρεάν εξομοιωτής ανοιχτού κώδικα (Quick EMUlator). Μιμείται τον επεξεργαστή του μηχανήματος μέσω δυναμικής δυαδικής μετάφρασης και παρέχει ένα σύνολο διαφορετικών μοντέλων υλικού

το υποστηριζόμενο περιβάλλον ολοκληρωμένης ανάπτυξης (integrated development environment / IDE) της Google ήταν το Eclipse χρησιμοποιώντας την προσθήκη Εργαλείων ανάπτυξης Android (Android Development Tools / ADT). Τον Δεκέμβριο του 2014, η Google κυκλοφόρησε το Android Studio, βασισμένο στο IntelliJ IDEA, ως το κύριο IDE για την ανάπτυξη εφαρμογών Android. Άλλα εργαλεία ανάπτυξης είναι διαθέσιμα, συμπεριλαμβανομένου ενός κιτ εγγενούς ανάπτυξης (native development kit / NDK) για εφαρμογές ή επεκτάσεις σε C ή C++, Google App Inventor, ένα οπτικό περιβάλλον για αρχάριους προγραμματιστές και διάφορα πλαίσια εφαρμογών ιστού για κινητές συσκευές πολλαπλών πλατφορμών. Τον Ιανουάριο του 2014, η Google αποκάλυψε ένα πλαίσιο βασισμένο στο Apache Cordova για τη μεταφορά εφαρμογών ιστού Chrome HTML 5 στο Android, τυλιγμένο σε ένα κέλυφος εγγενούς εφαρμογής. Επιπλέον, το Firebase εξαγοράστηκε από την Google το 2014 που παρέχει χρήσιμα εργαλεία για προγραμματιστές εφαρμογών και ιστού (Amer & El-Sappagh, 2022).

Το Android διαθέτει μια αυξανόμενη επιλογή από εφαρμογές τρίτων, τις οποίες μπορούν να αποκτήσουν οι χρήστες με λήψη και εγκατάσταση του αρχείου APK (πακέτο εφαρμογής Android) της εφαρμογής ή με λήψη τους χρησιμοποιώντας ένα πρόγραμμα αποθήκευσης εφαρμογών που επιτρέπει στους χρήστες να εγκαταστήσουν, να ενημερώσουν και να αφαιρέσουν εφαρμογές από τις συσκευές τους (Britannica/Android operating system, 2022).

Το Google Play Store είναι το κύριο κατάστημα εφαρμογών που είναι εγκατεστημένο σε συσκευές Android που συμμορφώνονται με τις απαιτήσεις συμβατότητας της Google και αδειοδοτούν το λογισμικό Google Mobile Services. Το Google Play Store επιτρέπει στους χρήστες να περιηγούνται, να κατεβάζουν και να ενημερώνουν εφαρμογές που δημοσιεύονται από την Google και τρίτους προγραμματιστές. Από τον Ιανουάριο του 2021, υπάρχουν περισσότερες από τρία εκατομμύρια εφαρμογές διαθέσιμες για Android στο Play Store, ενώ από τον Ιούλιο του 2013, είχαν πραγματοποιηθεί 50 δισεκατομμύρια εγκαταστάσεις εφαρμογών. Ορισμένες εταιρείες κινητής τηλεφωνίας προσφέρουν απευθείας χρέωση μέσω κινητού τηλεφώνου για αγορές εφαρμογών Google Play, όπου το κόστος της εφαρμογής προστίθεται στον μηνιαίο λογαριασμό του χρήστη. Από τον Μάιο του 2017 , υπάρχουν πάνω από ένα δισεκατομμύριο ενεργοί χρήστες το μήνα για

και συσκευών για το μηχάνημα, επιτρέποντάς του να εκτελεί μια ποικιλία επισκεπτών λειτουργικών συστημάτων.

το Gmail, το Android, το Chrome, το Google Play και τους Χάρτες (Tang, Li, Jiang, Gu, & Li, 2022).

Λόγω της ανοιχτής φύσης του Android, υπάρχουν επίσης διάφορες αγορές εφαρμογών τρίτων για το Android, είτε για να παρέχουν ένα υποκατάστατο για συσκευές που δεν επιτρέπεται να αποστέλλονται με το Google Play Store, είτε για να παρέχουν εφαρμογές που δεν μπορούν να προσφερθούν στο Google Play Store λόγω παραβιάσεων πολιτικής ή για άλλους λόγους. Παραδείγματα αυτών των καταστημάτων τρίτων είναι το Amazon Appstore, το GetJar και το SlideMe. Το F-Droid , μια άλλη εναλλακτική αγορά, επιδιώκει να παρέχει μόνο εφαρμογές που διανέμονται υπό άδειες δωρεάν και ανοιχτού κώδικα.

Τον Οκτώβριο του 2020, η Google αφαίρεσε αρκετές εφαρμογές Android από το Play Store, καθώς διαπιστώθηκε ότι παραβιάζουν τους κανόνες συλλογής δεδομένων της. Η εταιρεία ενημερώθηκε από το Διεθνές Συμβούλιο Ψηφιακής Λογοδοσίας (International Digital Accountability Council / IDAC) ότι εφαρμογές για παιδιά όπως το Number Coloring, το Princess Salon και το Cats & Cosplay, με συλλογικές λήψεις 20 εκατομμυρίων, παραβίαζαν τις πολιτικές της Google.

Στην εκδήλωση ανακοίνωσης των Windows 11 τον Ιούνιο του 2021, η Microsoft παρουσίασε το νέο Υποσύστημα Windows για Android (Windows Subsystem for Android / WSA) που θα επιτρέψει την υποστήριξη για το Android Open Source Project (AOSP) και θα επιτρέπει στους χρήστες να εκτελούν εφαρμογές Android στην επιφάνεια εργασίας των Windows (Bhatt & Furia, 2022).

4.3.1 Αποθήκευση

Η αποθήκευση συσκευών Android μπορεί να επεκταθεί χρησιμοποιώντας δευτερεύουσες συσκευές όπως κάρτες SD. Το Android αναγνωρίζει δύο τύπους δευτερεύοντος αποθηκευτικού χώρου: φορητό αποθηκευτικό χώρο (που χρησιμοποιείται από προεπιλογή) και αποθηκευτικό χώρο που μπορεί να προσαρμοστεί. Ο φορητός χώρος αποθήκευσης αντιμετωπίζεται ως εξωτερική συσκευή αποθήκευσης. Ο αποθηκευτικός χώρος που υιοθετείται, που εισήχθη στο Android 6.0, επιτρέπει στον εσωτερικό χώρο αποθήκευσης της συσκευής να εκτείνεται με την κάρτα SD, αντιμετωπίζοντάς τον ως επέκταση του εσωτερικού χώρου αποθήκευσης. Αυτό έχει το μειονέκτημα ότι εμποδίζει τη χρήση της κάρτας μνήμης με άλλη συσκευή, εκτός εάν διαμορφωθεί ξανά (Bhatt & Furia, 2022).

Το Android 4.4 παρουσίασε το Storage Access Framework (SAF), ένα σύνολο API για την πρόσβαση σε αρχεία στο σύστημα αρχείων της συσκευής. Από το Android 11, το Android

απαιτεί από τις εφαρμογές να συμμορφώνονται με μια πολιτική απορρήτου δεδομένων, γνωστή ως scoped storage, σύμφωνα με την οποία οι εφαρμογές μπορούν να έχουν αυτόματα πρόσβαση μόνο σε ορισμένους καταλόγους (όπως αυτούς για φωτογραφίες, μουσική και βίντεο) και εφαρμογές -συγκεκριμένους καταλόγους που έχουν δημιουργήσει οι ίδιοι. Οι εφαρμογές πρέπει να χρησιμοποιούν το SAF για πρόσβαση σε οποιοδήποτε άλλο τμήμα του συστήματος αρχείων (Amer & El-Sappagh, 2022).

4.3.2 Διαχείριση μνήμης

Δεδομένου ότι οι συσκευές Android συνήθως λειτουργούν με μπαταρίες, το Android έχει σχεδιαστεί για να διαχειρίζεται διαδικασίες για να διατηρεί την κατανάλωση ενέργειας στο ελάχιστο. Όταν μια εφαρμογή δεν χρησιμοποιείται, το σύστημα αναστέλλει τη λειτουργία της έτσι ώστε, ενώ είναι διαθέσιμη για άμεση χρήση αντί για κλειστή, να μην χρησιμοποιεί ισχύ μπαταρίας ή πόρους CPU. Το Android διαχειρίζεται αυτόματα τις εφαρμογές που είναι αποθηκευμένες στη μνήμη: όταν η μνήμη είναι χαμηλή, το σύστημα θα αρχίσει αόρατα και θα κλείνει αυτόματα τις ανενεργές διεργασίες, ξεκινώντας από εκείνες που ήταν ανενεργές για το μεγαλύτερο χρονικό διάστημα. Το Lifehacker ανέφερε το 2011 ότι οι εφαρμογές εξόντωσης εργασιών τρίτων έκαναν περισσότερο κακό παρά καλό (Amer & El-Sappagh, 2022).

4.3.3 Επιλογές ανάπτυξης

Ορισμένες ρυθμίσεις για χρήση από προγραμματιστές για εντοπισμό σφαλμάτων και ισχυρούς χρήστες βρίσκονται σε ένα υπομενού «Επιλογές προγραμματιστή», όπως η δυνατότητα επισήμανσης ενημερωμένων τμημάτων της οθόνης, εμφάνισης επικάλυψης με την τρέχουσα κατάσταση της οθόνης αφής, εμφάνισης σημείων επαφής για πιθανή χρήση στη μετάδοση οθόνης, ειδοποίηση του χρήστη για διαδικασίες παρασκηνίου, που δεν ανταποκρίνονται με την επιλογή τερματισμού τους («Εμφάνιση όλων των ANR», π.χ. «Η εφαρμογή δεν ανταποκρίνεται»), αποτροπή ενός χρήστη από τον έλεγχο της έντασης του συστήματος («Απενεργοποίηση απόλυτης έντασης ήχου») και προσαρμογή της διάρκειας των κινούμενων εικόνων μετάβασης ή απενεργοποίηση για επιτάχυνση της πλοήγησης (Amer & El-Sappagh, 2022).

Οι επιλογές προγραμματιστή είναι αρχικά κρυφές από το Android 4.2 «Jelly Bean», αλλά μπορούν να ενεργοποιηθούν ενεργοποιώντας τον αριθμό έκδοσης του λειτουργικού συστήματος στις πληροφορίες της συσκευής επτά φορές. Η απόκρυψη των επιλογών προγραμματιστή και πάλι απαιτεί τη διαγραφή των δεδομένων χρήστη για την εφαρμογή «Ρυθμίσεις», πιθανώς την επαναφορά κάποιων άλλων προτιμήσεων.

4.4 Ασφάλεια και ιδιωτικότητα

Το 2020, η Google ξεκίνησε την Πρωτοβουλία ευπάθειας συνεργατών Android για να βελτιώσει την ασφάλεια του Android και σχημάτισαν, επίσης, μια ομάδα ασφαλείας Android.

4.4.1 Τεχνικά χαρακτηριστικά ασφαλείας

Οι εφαρμογές Android εκτελούνται σε ένα sandbox, μια απομονωμένη περιοχή του συστήματος που δεν έχει πρόσβαση στους υπόλοιπους πόρους του συστήματος, εκτός εάν τα δικαιώματα πρόσβασης παραχωρούνται ρητά από τον χρήστη κατά την εγκατάσταση της εφαρμογής, ωστόσο αυτό μπορεί να μην είναι δυνατό για προ-εγκατεστημένες εφαρμογές. Δεν είναι δυνατό, για παράδειγμα, να απενεργοποιηθεί η πρόσβαση μικροφώνου της προεγκατεστημένης εφαρμογής κάμερας χωρίς να απενεργοποιηθεί εντελώς η κάμερα. Αυτό ισχύει και στις εκδόσεις Android 7 και 8 (Mia, και συν., 2022).

Από τον Φεβρουάριο του 2012, η Google χρησιμοποιεί τον σαρωτή κακόβουλου λογισμικού Google Bouncer για την παρακολούθηση και τη σάρωση εφαρμογών που είναι διαθέσιμες στο Google Play store. Μια λειτουργία «Επαλήθευση εφαρμογών» εισήχθη τον Νοέμβριο του 2012, ως μέρος της έκδοσης λειτουργικού συστήματος Android 4.2 «Jelly Bean», για τη σάρωση όλων των εφαρμογών, τόσο από το Google Play όσο και από πηγές τρίτων, για κακόβουλες συμπεριφορές. Αρχικά μόνο κατά τη διάρκεια της εγκατάστασης, το Verify Apps έλαβε μια ενημέρωση το 2014 για «συνεχή» σάρωση εφαρμογών και το 2017 η λειτουργία έγινε ορατή στους χρήστες μέσω ενός μενού στις Ρυθμίσεις (Mia, και συν., 2022).

Πριν εγκατασταθεί μια εφαρμογή, το κατάστημα Google Play εμφανίζει μια λίστα με τις απαιτήσεις που χρειάζεται μια εφαρμογή για να λειτουργήσει. Αφού ελέγξει αυτές τις άδειες, ο χρήστης μπορεί να επιλέξει να τις αποδεχτεί ή να τις αρνηθεί, εγκαθιστώντας την εφαρμογή μόνο εάν αποδεχτεί. Στο Android 6.0 «Marshmallow», το σύστημα αδειών άλλαξε. Στις εφαρμογές δεν εκχωρούνται πλέον αυτόματα όλα τα καθορισμένα δικαιώματα κατά την εγκατάσταση. Αντ' αυτού χρησιμοποιείται ένα σύστημα επιλογής, στο οποίο οι χρήστες καλούνται να παραχωρήσουν ή να αρνηθούν μεμονωμένα δικαιώματα σε μια εφαρμογή όταν χρειάζονται για πρώτη φορά. Οι εφαρμογές θυμούνται τις εξουσιοδοτήσεις που έχουν λάβει, οι οποίες μπορούν να ανακληθούν από τον χρήστη ανά πάσα στιγμή. Ωστόσο, οι προεγκατεστημένες εφαρμογές δεν αποτελούν πάντα μέρος αυτής της προσέγγισης. Σε ορισμένες περιπτώσεις, ενδέχεται να μην είναι

δυνατή η άρνηση ορισμένων αδειών σε προεγκατεστημένες εφαρμογές, ούτε η απενεργοποίησή τους. Δεν είναι δυνατή η απεγκατάσταση ή η απενεργοποίηση της εφαρμογής Υπηρεσίες Google Play . Οποιαδήποτε προσπάθεια αναγκαστικής διακοπής, έχει ως αποτέλεσμα την επανεκκίνηση της εφαρμογής από μόνη της. Τα δικαιώματα εξακολουθούν να μπορούν να ανακληθούν για αυτές τις εφαρμογές, αν και αυτό μπορεί να εμποδίσει τη σωστή λειτουργία τους και εμφανίζεται μια προειδοποίηση για το σκοπό αυτό (Kong, Zhang, Guo, Han, & Long, 2022).

Τον Σεπτέμβριο του 2014, ο Jason Nova του Android Authority ανέφερε μια μελέτη της γερμανικής εταιρείας ασφαλείας Fraunhofer AISEC σε λογισμικό προστασίας από ιούς και απειλές κακόβουλου λογισμικού στο Android. Συγκεκριμένα, έγραψε ότι «Το λειτουργικό σύστημα Android ασχολείται με πακέτα λογισμικού τοποθετώντας τα σε sandbox. Αυτό δεν επιτρέπει στις εφαρμογές να παραθέσουν τα περιεχόμενα του καταλόγου άλλων εφαρμογών για να διατηρηθεί το σύστημα ασφαλές. Με το να μην επιτρέπει στο πρόγραμμα προστασίας από ιούς να παραθέτει τους καταλόγους άλλων εφαρμογών μετά την εγκατάσταση, οι εφαρμογές που δεν εμφανίζουν εγγενή ύποπτη συμπεριφορά κατά τη λήψη διαγράφονται ως ασφαλείς. Εάν στη συνέχεια ενεργοποιηθούν τμήματα της εφαρμογής που αποδειχθούν κακόβουλα, το πρόγραμμα προστασίας από ιούς δεν θα έχει κανέναν τρόπο να το μάθει, καθώς βρίσκεται εντός της εφαρμογής και εκτός του προγράμματος προστασίας από ιούς» (Kong, Zhang, Guo, Han, & Long, 2022).

Επίσης, αποκαλύφθηκε ότι οι δοκιμασμένες εφαρμογές προστασίας από ιούς δεν παρέχουν προστασία από προσαρμοσμένο κακόβουλο λογισμικό ή στοχευμένες επιθέσεις και ότι οι δοκιμασμένες εφαρμογές προστασίας από ιούς δεν είναι επίσης σε θέση να εντοπίσουν κακόβουλο λογισμικό που είναι εντελώς άγνωστο μέχρι σήμερα, αλλά δεν καταβάλλει καμία προσπάθεια να κρύψει την κακοήθεια του».

Τον Αύγουστο του 2013, η Google ανακοίνωσε το Android Device Manager (μετονομάστηκε Find My Device τον Μάιο του 2017), μια υπηρεσία που επιτρέπει στους χρήστες να παρακολουθούν, να εντοπίζουν και να εκκαθαρίζουν (format) εξ αποστάσεως τη συσκευή τους Android. Τον Δεκέμβριο του 2016, η Google παρουσίασε μια εφαρμογή «Αξιόπιστες Επαφές», επιτρέποντας στους χρήστες να ζητούν παρακολούθηση τοποθεσίας αγαπημένων προσώπων κατά τη διάρκεια έκτακτης ανάγκης. Το 2020, οι Αξιόπιστες Επαφές τερματίστηκαν και η λειτουργία κοινής χρήσης τοποθεσίας μπήκε στους Χάρτες Google (Mia, και συν., 2022).

Στις 8 Οκτωβρίου 2018, η Google ανακοίνωσε νέες απαιτήσεις του καταστήματος Google Play για την καταπολέμηση της υπερβολικής κοινής χρήσης δυνητικά ευαίσθητων πληροφοριών, συμπεριλαμβανομένων των αρχείων καταγραφής κλήσεων και μηνυμάτων κειμένου. Το ζήτημα προκύπτει από το γεγονός ότι πολλές εφαρμογές ζητούν άδειες πρόσβασης στα προσωπικά στοιχεία των χρηστών (ακόμα και αν αυτές οι πληροφορίες δεν χρειάζονται για τη λειτουργία της εφαρμογής) και ορισμένοι χρήστες αναμφισβήτητα χορηγούν αυτές τις άδειες. Εναλλακτικά, μια άδεια μπορεί να αναφέρεται στο Manifest[5] της Android εφαρμογής όπως απαιτείται (σε αντίθεση με το προαιρετικό) και η εφαρμογή δεν θα εγκατασταθεί εκτός εάν ο χρήστης χορηγήσει την άδεια. Οι χρήστες μπορούν να αποσύρουν οποιαδήποτε, ακόμη και απαιτούμενη, άδεια από οποιαδήποτε εφαρμογή στις ρυθμίσεις της συσκευής μετά την εγκατάσταση της εφαρμογής, αλλά λίγοι χρήστες το κάνουν αυτό. Η Google υποσχέθηκε να συνεργαστεί με προγραμματιστές και να δημιουργήσει εξαιρέσεις εάν οι εφαρμογές τους απαιτούν άδειες τηλεφώνου ή SMS για «βασική λειτουργικότητα εφαρμογής». Η απαίτηση επιπέδου API μπορεί να καταπολεμήσει την πρακτική των προγραμματιστών εφαρμογών να παρακάμπτουν ορισμένες οθόνες αδειών καθορίζοντας τις πρώιμες εκδόσεις Android που είχαν ένα πιο χονδροειδές μοντέλο άδειας (Kong, Zhang, Guo, Han, & Long, 2022).

Θα πρέπει να αποφεύγονται τα δικαιώματα εφαρμογής που δεν είναι απαραίτητα για να λειτουργήσει μια εφαρμογή. Εάν η εφαρμογή δεν χρειάζεται πρόσβαση σε κάτι -όπως η κάμερα ή η τοποθεσία του χρήστη- τότε δεν πρέπει να το επιτρέψει. Να λαμβάνεται υπόψη το απόρρητο όταν αποφασίζει ο χρήστης εάν θα αποφύγει ή θα αποδεχτεί ένα αίτημα άδειας εφαρμογής.

Οι άδειες συστήματος Android χωρίζονται σε «κανονικές" και «επικίνδυνες» άδειες. Το Android επιτρέπει «κανονικές» άδειες -όπως η παροχή πρόσβασης σε εφαρμογές στο διαδίκτυο- από προεπιλογή. Αυτό συμβαίνει επειδή οι κανονικές άδειες δεν θα πρέπει να θέτουν σε κίνδυνο το απόρρητό του εκάστοτε χρήστη ή τη λειτουργικότητα της συσκευής του.

Για τις λεγόμενες «επικίνδυνες» άδειες, το Android απαιτεί την άδειά του χρήστη για να τις αποκτήσει. Αυτές οι «επικίνδυνες» άδειες περιλαμβάνουν πρόσβαση στο ιστορικό

[5] Κάθε έργο εφαρμογής πρέπει να έχει ένα AndroidManifest.xmlαρχείο, με αυτό ακριβώς το όνομα, στη ρίζα του συνόλου προέλευσης του έργου. Το αρχείο δήλωσης περιγράφει βασικές πληροφορίες σχετικά με την εφαρμογή στα εργαλεία κατασκευής Android, στο λειτουργικό σύστημα Android και στο Google Play.

κλήσεων, τα προσωπικά μηνύματα, την τοποθεσία, την κάμερα, το μικρόφωνο και πολλά άλλα. Αυτές οι άδειες δεν είναι εγγενώς επικίνδυνες, αλλά έχουν τη δυνατότητα κακής χρήσης με αρνητικές συνέπειες για την ιδιωτικότητα και την προστασία προσωπικών δεδομένων των χρηστών. Γι' αυτό το Android δίνει την ευκαιρία να τα αποδεχτεί ή να τα αρνηθεί ο εκάστοτε χρήστης.

Ορισμένες εφαρμογές χρειάζονται αυτές τις άδειες για να λειτουργήσουν κανονικά. Σε αυτές τις περιπτώσεις, πρέπει να ελέγχεται ότι μια εφαρμογή είναι ασφαλής προτού εγκατασταθεί και να βεβαιωθεί ο εκάστοτε χρήστης ότι η εφαρμογή προέρχεται από έναν αξιόπιστο προγραμματιστή (AVG / App Permissions on Android, 2023). Ωστόσο, ζητήματα προστασίας προσωπικών δεδομένων εγείρονται αν ζητούνται τέτοιες άδειες χωρίς να είναι πραγματικά απαραίτητο για τη λειτουργία της εφαρμογής ή αν γίνεται αξιοποίηση τέτοιων αδειών για άλλους, μη διαφανείς προς το χρήστη, σκοπούς.

4.4.2 Συνήθεις απειλές για την ασφάλεια

Έρευνα από την εταιρεία ασφαλείας Trend Micro αναφέρει την κατάχρηση υπηρεσιών premium ως τον πιο κοινό τύπο κακόβουλου λογισμικού Android, όπου μηνύματα κειμένου αποστέλλονται από μολυσμένα τηλέφωνα σε αριθμούς τηλεφώνου υψηλής ποιότητας χωρίς τη συγκατάθεση ή ακόμη και τη γνώση του χρήστη. Άλλο κακόβουλο λογισμικό εμφανίζει ανεπιθύμητες και παρεμβατικές διαφημίσεις στη συσκευή ή στέλνει προσωπικές πληροφορίες σε μη εξουσιοδοτημένα τρίτα μέρη. Οι απειλές για την ασφάλεια στο Android φέρεται να αυξάνονται εκθετικά. Ωστόσο, οι μηχανικοί της Google υποστήριξαν ότι η απειλή κακόβουλου λογισμικού και ιών στο Android γίνεται υπερβολική από τις εταιρείες ασφαλείας για εμπορικούς λόγους και έχουν κατηγορήσει τη βιομηχανία ασφάλειας ότι εκμεταλλεύεται τον φόβο των χρηστών για να πουλήσει λογισμικό προστασίας από ιούς στους χρήστες. Η Google υποστηρίζει ότι το επικίνδυνο κακόβουλο λογισμικό είναι στην πραγματικότητα εξαιρετικά σπάνιο και μια έρευνα που διεξήχθη από την F-Secure έδειξε ότι μόνο το 0,5% του κακόβουλου λογισμικού Android που αναφέρθηκε προήλθε από το Google Play store (Kong, Zhang, Guo, Han, & Long, 2022).

Το 2021, δημοσιογράφοι και ερευνητές ανέφεραν την ανακάλυψη του spyware, ονόματι Pegasus, που αναπτύχθηκε και διανεμήθηκε από μια ιδιωτική εταιρεία, το οποίο μπορεί και έχει χρησιμοποιηθεί για να μολύνει smartphones iOS και Android συχνά – εν μέρει μέσω χρήσης 0-day exploit – χωρίς την ανάγκη οποιασδήποτε αλληλεπίδρασης χρήστη ή χωρίς σημαντικές ενδείξεις για τον χρήστη και για την εξαγωγή δεδομένων, την

παρακολούθηση τοποθεσιών των χρηστών και την ενεργοποίηση του μικροφώνου ανά πάσα στιγμή. Η ανάλυση της κυκλοφορίας δεδομένων από δημοφιλή smartphone που εκτελούν παραλλαγές του Android διαπίστωσε σημαντική από προεπιλογή συλλογή και κοινή χρήση δεδομένων χωρίς εξαίρεση από αυτό το προεγκατεστημένο λογισμικό. Και τα δύο αυτά ζητήματα δεν αντιμετωπίζονται ή δεν μπορούν να αντιμετωπιστούν με ενημερώσεις κώδικα ασφαλείας (Kong, Zhang, Guo, Han, & Long, 2022).

4.4.3 Εντοπισμός τοποθεσίας

Τα smartphone Android έχουν τη δυνατότητα να αναφέρουν τη θέση των σημείων πρόσβασης Wi-Fi, που συναντώνται καθώς οι χρήστες τηλεφώνων μετακινούνται, για να δημιουργήσουν βάσεις δεδομένων που περιέχουν τις φυσικές τοποθεσίες εκατοντάδων εκατομμυρίων τέτοιων σημείων πρόσβασης. Αυτές οι βάσεις δεδομένων σχηματίζουν ηλεκτρονικούς χάρτες για τον εντοπισμό smartphone, επιτρέποντάς τους να εκτελούν εφαρμογές όπως το Foursquare, το Google Latitude, το Facebook Places και να παρέχουν διαφημίσεις βάσει τοποθεσίας. Λογισμικό παρακολούθησης τρίτων, όπως το TaintDroid, ένα έργο που χρηματοδοτείται από ακαδημαϊκή έρευνα, μπορεί, σε ορισμένες περιπτώσεις, να ανιχνεύσει πότε αποστέλλονται προσωπικές πληροφορίες από εφαρμογές σε απομακρυσμένους διακομιστές (Kong, Zhang, Guo, Han, & Long, 2022).

4.4.4 Ιχνηλάτες (Trackers)

Το Tracker, είναι ένα κομμάτι λογισμικού, του οποίου η αποστολή είναι να συλλέγει πληροφορίες σχετικά με το άτομο που χρησιμοποιεί την εφαρμογή, τον τρόπο με τον οποίο τη χρησιμοποιεί ή για το smartphone που χρησιμοποιείται. Ένα tracker διανέμεται συνήθως από εταιρείες ως SDK (Software Development Kit), ένα είδος έτοιμου κιτ εργαλείων, με στόχο να διευκολύνει τους προγραμματιστές των εφαρμογών. Πρέπει να σημειωθεί: υπάρχουν trackers «ανοιχτού κώδικα», ο κώδικας τους είναι διαθέσιμος και ανοιχτός σε όλους (Skyfii /Smartphone tracking, 2020).

1. Η ενεργή παρακολούθηση smartphone με χρήση GSM, 3G ή 4G είναι παράνομη στις περισσότερες χώρες. Όλες οι άλλες μέθοδοι ενεργής παρακολούθησης smartphone απαιτούν συμμετοχή χρήστη ως εξής:
    - Bluetooth Beacons: ο χρήστης πρέπει να έχει εγκατεστημένη την εφαρμογή για κινητά στο τηλέφωνό του και να αποδέχεται τις σχετικές άδειες.
    - WiFi : ο χρήστης πρέπει να συνδεθεί στο δίκτυο WiFi
    - GPS: ο χρήστης πρέπει να κατεβάσει και να εγκαταστήσει μια εφαρμογή με τα σχετικά δικαιώματα.

2. Η παθητική παρακολούθηση smartphone δεν απαιτεί εφαρμογή για κινητά ή συμμετοχή χρήστη και παρέχει μόνο ανώνυμα δεδομένα και μπορεί να γίνει με τους ακόλουθους τρόπους:

   - Παρακολούθηση τηλεφώνου GSM, 3G, 4G, 5G: απαιτείται πολύ εξειδικευμένο υλικό και λογισμικό.
   - Παρακολούθηση τηλεφώνου Bluetooth: – λόγω του πρωτοκόλλου «χειραψίας» της συσκευής του Bluetooth, απαιτείται μη τυποποιημένο υλικό για μηνύματα Bluetooth (δηλαδή ένα dongle Ubertooth).
   - Παρακολούθηση τηλεφώνου WiFi: – τα smartphone εκπέμπουν ανιχνευτές WiFi σε αναζήτηση συνδέσεων δικτύου WiFi συνεχώς και η υποκλοπή αυτών των ανιχνευτών είναι σχετικά εύκολη.

4.4.5 Περαιτέρω δικλείδες ασφαλείας

Το 2018, η νορβηγική εταιρεία ασφαλείας Promon ανακάλυψε μια σοβαρή έλλειψη ασφαλείας Android που μπορεί να χρησιμοποιηθεί για την κλοπή διαπιστευτηρίων σύνδεσης, πρόσβασης μηνυμάτων και παρακολούθησης τοποθεσίας, τα οποία θα μπορούσαν να βρεθούν σε όλες τις εκδόσεις του Android, συμπεριλαμβανομένου του Android 10. Η ευπάθεια προέκυψε με την εκμετάλλευση ενός σφάλματος στο σύστημα πολλαπλών εργασιών που επιτρέπει σε μια κακόβουλη εφαρμογή να επικαλύπτει νόμιμες εφαρμογές με ψεύτικες οθόνες σύνδεσης που οι χρήστες δεν γνωρίζουν όταν παραδίδουν διαπιστευτήρια ασφαλείας. Οι χρήστες μπορούν επίσης να εξαπατηθούν ώστε να παραχωρήσουν πρόσθετες άδειες στις κακόβουλες εφαρμογές, οι οποίες αργότερα τους επιτρέπουν να εκτελούν διάφορες κακόβουλες δραστηριότητες, όπως υποκλοπή μηνυμάτων ή κλήσεων και κλοπή τραπεζικών διαπιστευτηρίων. Το δίκτυο Avast Threat Labs ανακάλυψε επίσης ότι πολλές προεγκατεστημένες εφαρμογές σε αρκετές εκατοντάδες νέες συσκευές Android περιέχουν επικίνδυνο κακόβουλο λογισμικό και adware. Κάποιο από το προεγκατεστημένο κακόβουλο λογισμικό μπορεί να διαπράξει απάτη σε διαφημίσεις ή ακόμη και να καταλάβει τη συσκευή υποδοχής του (Mia, και συν., 2022).

Το 2020, το consumer watchdog[6] ανέφερε ότι περισσότερες από ένα δισεκατομμύριο συσκευές Android που κυκλοφόρησαν το 2012 ή νωρίτερα, που ήταν το 40% των συσκευών Android παγκοσμίως, κινδύνευαν να παραβιαστούν. Αυτό το συμπέρασμα

[6] Consumer Watchdog / Υπηρεσία Παρακολούθησης Καταναλωτών (https://consumerwatchdog.org/mobile/).

προέκυψε από το γεγονός ότι δεν εκδόθηκαν ενημερώσεις ασφαλείας για τις εκδόσεις Android κάτω από το 7.0 το 2019. Επίσης, συνεργάστηκε με το εργαστήριο προστασίας από ιούς AV Comparatives για να μολύνει πέντε μοντέλα τηλεφώνων με κακόβουλο λογισμικό και πέτυχε σε κάθε περίπτωση (Kong, Zhang, Guo, Han, & Long, 2022).

Στις 5 Αυγούστου 2020, το Twitter δημοσίευσε ένα ιστολόγιο παροτρύνοντας τους χρήστες του να ενημερώσουν τις εφαρμογές τους στην πιο πρόσφατη έκδοση σχετικά με μια ανησυχία για την ασφάλεια που επέτρεπε σε άλλους να έχουν πρόσβαση σε απευθείας μηνύματα. Ένας χάκερ θα μπορούσε εύκολα να χρησιμοποιήσει τις «άδειες συστήματος Android» για να πάρει τα διαπιστευτήρια του λογαριασμού για να το κάνει. Το ζήτημα ασφαλείας αφορά μόνο το Android 8 (Android Oreo) και το Android 9 (Android Pie). Μάλιστα, το Twitter επιβεβαίωσε ότι η ενημέρωση της εφαρμογής θα περιορίσει τέτοιες πρακτικές (Mia, και συν., 2022).

Κεφάλαιο 5

Σχεδιαστική προσέγγιση «data protection by design» και «data protection by default» Εφαρμογών Android: υγείας από κρατικούς φορείς

Στο παρόν κεφάλαιο παρουσιάζεται η σχεδιαστική προσέγγιση «data protection by design», δηλαδή τους κανονισμούς απορρήτου και προστασίας δεδομένων για τις εφαρμογές mHealth στην ΕΕ, την προστασία δεδομένων σε εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές, την ελαχιστοποίηση δεδομένων σε εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές, τις ποινές και πρόστιμα για μη συμμόρφωση με τον GDPR και τις συστάσεις προς κατασκευαστές εφαρμογών για κινητά σε οργανισμούς υγειονομικής περίθαλψης. Και τέλος αναλύεται η προστασία δεδομένων από προεπιλογή / «data protection by default» εφαρμογών Android υγείας από κρατικούς φορείς.

5.1 Data Protection by Design εφαρμογών Android υγείας από κρατικούς φορείς

Υπάρχουν πολλοί κανονισμοί απορρήτου και προστασίας δεδομένων που πρέπει να τηρούν οι οργανισμοί υγειονομικής περίθαλψης όσον αφορά τις Προστατευμένες Πληροφορίες Υγείας (Protected Health Information / PHI) και τις Ηλεκτρονικές Προστατευόμενες Πληροφορίες Υγείας (Electronic Protected Health Information / ePHI). Στην Ευρώπη, η προστασία δεδομένων και το απόρρητο των PHI και ePHI διέπονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

5.1.1 Κανονισμοί απορρήτου και προστασίας δεδομένων για τις εφαρμογές mHealth στην ΕΕ

Όλες οι πληροφορίες ασθενών που συλλέγονται στην Ευρωπαϊκή Ένωση υπόκεινται στον GDPR. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων είναι, όπως

προαναφέρθηκε, ένας Κανονισμός της Ευρωπαϊκής Ένωσης που διέπει την προστασία των δεδομένων και το απόρρητο. Δημιουργήθηκε για την προστασία των προσωπικών στοιχείων των φυσικών προσώπων και την προάσπιση των δικαιωμάτων τους, θέτοντας υποχρεώσεις σε εταιρείες, οργανισμούς και κρατικές υπηρεσίες σε υψηλότερο επίπεδο όσον αφορά τη συλλογή, αποθήκευση και χρήση προσωπικών δεδομένων. Ειδικά όσον αφορά τις εφαρμογές για κινητά (συμπεριλαμβανομένων των εφαρμογών mHealth), ο GDPR επιβάλλει τρεις συνεχείς απαιτήσεις. Είναι (European Commission/Privacy code of conduct on mobile health apps, 2021):

1. η προστασία δεδομένων,
2. η ελαχιστοποίηση δεδομένων και
3. το απόρρητο από το σχεδιασμό.

5.1.2 Προστασία δεδομένων σε εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές

Προκειμένου να διασφαλιστεί ικανοποιητική προστασία δεδομένων στις εφαρμογές mHealth, οι κατασκευαστές εφαρμογών θα πρέπει πρώτα να διασφαλίσουν τον ασφαλή έλεγχο ταυτότητας της εφαρμογής. Η πρόσβαση σε εφαρμογές υγείας για κινητά θα πρέπει τουλάχιστον να απαιτεί από έναν ασθενή να εισάγει το όνομα χρήστη και τον κωδικό πρόσβασής του κάθε φορά που ανοίγει την εφαρμογή. Οι εφαρμογές θα πρέπει επίσης να αποσυνδέουν έναν ασθενή μετά από ορισμένο χρόνο μη χρήσης. Κατά προτίμηση, οι εφαρμογές mHealth θα πρέπει επίσης να χρησιμοποιούν βιομετρικό έλεγχο ταυτότητας (FaceID ή TouchID) ή έλεγχο ταυτότητας πολλαπλών παραγόντων για την επίτευξη υψηλότερου επιπέδου ασφαλούς ελέγχου ταυτότητας (Machado, Cunha, & Jorge Gouveia, 2023).

Το δεύτερο στοιχείο προστασίας δεδομένων είναι η διασφάλιση ότι όλες οι πληροφορίες ασθενών, όχι μόνο οι προστατευμένες πληροφορίες υγείας, αποθηκεύονται κρυπτογραφημένες στην εφαρμογή. Οι κατασκευαστές εφαρμογών mHealth μπορούν να το επιτύχουν αυτό κρυπτογραφώντας το sandbox της εφαρμογής με ισχυρή κρυπτογράφηση (π.χ. AES-256[7]). Επιπλέον, οι συμβολοσειρές, οι πόροι, οι προτιμήσεις

[7] Το Advanced Encryption Standard (AES), είναι μια προδιαγραφή για την κρυπτογράφηση ηλεκτρονικών δεδομένων που καθιερώθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (National Institute of Standards and Technology / NIST) στο 2001

εντός εφαρμογής ενδέχεται επίσης να αποθηκεύουν δεδομένα ασθενούς, επομένως θα πρέπει επίσης να είναι κρυπτογραφημένα.

Τέλος, οι κατασκευαστές εφαρμογών θα πρέπει να διασφαλίζουν ότι η εφαρμογή υγείας για κινητά επικοινωνεί με διακομιστές υποστήριξης μέσω κρυπτογραφημένου καναλιού, έτσι ώστε τα δεδομένα ασθενών που αποστέλλονται ή λαμβάνονται να μην μπορούν να υποκλαπούν από επίθεση Man-in-the-Middle[8] ή άλλη επίθεση που βασίζεται στο δίκτυο. Επιπλέον, οι κατασκευαστές εφαρμογών θα πρέπει να λαμβάνουν μέτρα για την επικύρωση των ψηφιακών πιστοποιητικών (τόσο από την πλευρά του πελάτη όσο και από την πλευρά του διακομιστή) και να διασφαλίζουν την αυθεντικότητα των πιστοποιητικών και των CAs (Εκδότες Πιστοποιητικών) (Machado, Cunha, & Jorge Gouveia, 2023).

5.1.3 Ελαχιστοποίηση δεδομένων σε εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές

Η ελαχιστοποίηση δεδομένων βάσει του GDPR απαιτεί η επεξεργασία προσωπικών δεδομένων να είναι επαρκής, σχετική και περιορισμένη σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

5.1.4 Privacy by Design σε εφαρμογές Mobile Healthcare

Στον GDPR, ο όρος «Απόρρητο από τον σχεδιασμό» δεν σημαίνει τίποτα περισσότερο από «προστασία δεδομένων μέσω του σχεδιασμού τεχνολογίας». Αποτελεί ένα από τα πιο κρίσιμα και απαιτητικότερα μέρη του νόμου. Εν ολίγοις, το απόρρητο μέσω σχεδίασης σημαίνει ότι οι οργανισμοί και οι προγραμματιστές πρέπει να εφαρμόζουν «κατάλληλα τεχνικά μέτρα» που διασφαλίζουν την προστασία των δεδομένων και ενσωματώνουν «τις απαραίτητες διασφαλίσεις» στην επεξεργασία προσωπικών δεδομένων προκειμένου να πληρούν τις απαιτήσεις του GDPR και να προστατεύουν τα δικαιώματα των δεδομένων υποκείμενα (δηλαδή τους ασθενείς) (Galetsi, Katsaliaki, & Kumar, 2023).

Οι εφαρμογές υγείας για κινητές συσκευές συλλέγουν, καταγράφουν και αποθηκεύουν δεδομένα. Επιπλέον, οι εφαρμογές mHealth ανακτούν δεδομένα και μεταδίδουν δεδομένα σε διακομιστές cloud ή backend που ελέγχουν την υπηρεσία που παρέχεται από

[8] Στην κρυπτογραφία και την ασφάλεια υπολογιστών, person-in-the-middle (PITM) επίθεση είναι μια κυβερνοεπίθεση όπου ο εισβολέας κρυφά αναμεταδίδει και πιθανώς αλλάζει τις επικοινωνίες μεταξύ δύο μερών που πιστεύουν ότι επικοινωνούν απευθείας μεταξύ τους, καθώς ο εισβολέας έχει παρεμβληθεί μεταξύ των δύο μερών.

την εφαρμογή. Οι εφαρμογές έχουν επίσης αποθηκεύσει βαθιά μέσα στον κώδικα της ίδιας της εφαρμογής και στις προτιμήσεις της εφαρμογής, κρίσιμες πληροφορίες σχετικά με δίκτυα, χρήστες, προφίλ και υπηρεσίες που χρησιμοποιούνται από την εφαρμογή. Οι εφαρμογές είναι θησαυροί προσωπικών πληροφοριών και διαδρομές προς τα προσωπικά στοιχεία. Εξαιτίας αυτού, οι οργανισμοί υγειονομικής περίθαλψης πρέπει να προστατεύουν πλήρως τις εφαρμογές τους (με κρυπτογράφηση, obfuscation, app hardening / ανθεκτικότητα, προστασία jailbreak/root[9]), για να προστατεύουν τα δεδομένα ασθενών και τον πηγαίο κώδικα και τη λογική της εφαρμογής (Galetsi, Katsaliaki, & Kumar, 2023).

Επίσης, δεν πρέπει να συλλέγονται περισσότερα δεδομένα από ό,τι χρειάζεται για την επίτευξη του σκοπού της εφαρμογής – εκτός ίσως αν υπάρχει ελεύθερη, ρητή και σαφής συγκατάθεση του χρήστη (κατόπιν πλήρους ενημέρωσής του). Σε αυτήν την κατεύθυνση, κρίσιμο είναι να λαμβάνεται μέριμνα για την περίπτωση χρήσης βιβλιοθηκών από τρίτα μέρη (third party libraries): λόγω της αρχιτεκτονικής του Android, κάθε άδεια που εκχωρείται σε μία εφαρμογή συνεπάγεται αυτόματα και εκχώρησή της και στον πάροχο της βιβλιοθήκης αυτής, το οποίο συνεπάγεται μία επεξεργασία δεδομένων που πολλές φορές είναι υπέρμετρη και δεν συνάδει με την αρχή της ελαχιστοποίησης των δεδομένων. Συνεπώς, δεν είναι «αθώα» η χρήση μίας βιβλιοθήκης τρίτου μέλους και χρήζει προσοχής η επιλογή της, ακόμα και αν πρόκειται να εξυπηρετήσει θεμιτό σκοπό όπως, π.χ., η εξαγωγή στατιστικών.

5.1.5 Δικαίωμα στη λήθη στις εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές

Μια άλλη απαίτηση βάσει του GDPR είναι το δικαίωμα στη λήθη (άρθρο 17). Όταν μια εφαρμογή mHealth έχει γραφτεί με γνώμονα το απόρρητο λόγω του σχεδιασμού (obfuscation, κρυπτογράφηση, app hardening / ανθεκτικότητα, προστασία jailbreak/root), η συμμόρφωση με το άρθρο 17 μπορεί εύκολα να επιτευχθεί. Κατόπιν αιτήματος ενός ασθενούς να διαγράψει όλα τα προσωπικά του στοιχεία, ο οργανισμός υγειονομικής περίθαλψης μπορεί να διαγράψει τον λογαριασμό του ασθενούς (όνομα χρήστη, κωδικό πρόσβασης και όλα τα δεδομένα ασθενούς) από τον διακομιστή

[9] Το jailbreaking ή το rooting της συσκευής από τη φύση της παρέχει ένα επίπεδο πρόσβασης που μπορεί να χρησιμοποιηθεί για να εξαπατήσει κάθε προσπάθεια εντοπισμού της. Αυτή η προσθήκη προορίζεται να παρέχει ένα εύλογο επίπεδο ανίχνευσης που μπορεί να χρησιμοποιήσει η συσκευή για να προειδοποιήσει τους χρήστες ή να απενεργοποιήσει ορισμένες λειτουργίες.

υποστήριξης. Από εκείνη τη στιγμή, ο ασθενής δεν θα μπορεί πλέον να συνδεθεί στην εφαρμογή. Και εφόσον οι προγραμματιστές έχουν εφαρμόσει βέλτιστες πρακτικές ασφάλειας εφαρμογών για κινητά (δηλαδή: κρυπτογράφηση όλων των δεδομένων και «συσκότιση» / obfuscation του πηγαίου κώδικα, της λογικής και των πληροφοριών εντοπισμού σφαλμάτων), τότε καμία από τις πληροφορίες που ενδέχεται να παραμείνουν στην εφαρμογή δεν είναι προσβάσιμη χρησιμοποιώντας στατική ή δυναμική ανάλυση (Ahn & Park, 2022).

5.1.6 Ποινές και πρόστιμα για μη συμμόρφωση με τον GDPR

Ο GDPR έχει τους αυστηρότερους όρους από κάθε κανονισμό προστασίας της ιδιωτικής ζωής και των δεδομένων στον κόσμο. Τα πρόστιμα και οι ποινές για μη συμμόρφωση με τον GDPR μπορεί να φτάσουν τα 20 εκατομμύρια ευρώ (22 εκατομμύρια δολάρια ΗΠΑ) ή το 4% των ετήσιων εσόδων μιας εταιρείας (όποιο είναι υψηλότερο). Ως εκ τούτου, δεν αποτελεί έκπληξη το γεγονός ότι οι ειδικοί συμφωνούν ότι το GDPR θα μπορούσε είναι πολύ πιο σημαντικό από το HIPAA (Health Insurance Portability and Accountability Act)[10], όχι μόνο τιμωρητικά, αλλά και ως προς το εύρος. Για παράδειγμα, και όσον αφορά την αυστηρότητα των νόμων, σε αρκετούς παρόχους υγειονομικής περίθαλψης στη Σουηδία επιβλήθηκαν πρόστιμα πολλών εκατομμυρίων ευρώ για παραβιάσεις του GDPR (Li, και συν., 2023).

5.1.7 Συστάσεις προς κατασκευαστές εφαρμογών για κινητά σε οργανισμούς υγειονομικής περίθαλψης

Η διασφάλιση της συμμόρφωσης με τον GDPR και τον νόμο περί προστασίας δεδομένων είναι κρίσιμης σημασίας για τις εφαρμογές υγείας για κινητές συσκευές. Χρησιμοποιώντας ένα Αυτοματισμό Άμυνας Κυβερνοχώρου (όπως τα: Signifyd, SEON, SHIELD, Appdome, Sift, Kount, Emailage, ThreatMetrix, Cybersource) το οποίο θα προστατεύει, θα πιστοποιεί και θα παρακολουθεί απειλές και επιθέσεις εναντίον όλων των εφαρμογών για κινητά ακριβώς μέσα στη γραμμή CI/CD του DevOps, οι οργανισμοί

[10] Ο νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας του 1996 (Health Insurance Portability and Accountability Act / HIPAA) είναι ένας ομοσπονδιακός νόμος που απαιτούσε τη δημιουργία εθνικών προτύπων για την προστασία ευαίσθητων πληροφοριών υγείας των ασθενών από την αποκάλυψη χωρίς τη συγκατάθεση ή τη γνώση του ασθενούς. Το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών των ΗΠΑ (Health and Human Services / HHS) εξέδωσε τον Κανόνα Απορρήτου HIPAA για την εφαρμογή των απαιτήσεων του HIPAA. Ο Κανόνας ασφαλείας HIPAA προστατεύει ένα υποσύνολο πληροφοριών που καλύπτονται από τον Κανόνα απορρήτου (Health Insurance Portability and Accountability Act of 1996 (HIPAA), 1996).

υγειονομικής περίθαλψης μπορούν να ασφαλίσουν πλήρως τις εφαρμογές mHealth τους και να πληρούν όλους τους διαφορετικούς κανονισμούς σε όλο τον κόσμο. Οι Πλατφόρμες Ασφάλειας Εφαρμογών για Κινητά και Πρόληψης Απάτης πρέπει να ενσωματώνουν αυτόματα την ασφάλεια στις εφαρμογές για κινητά, χωρίς την ανάγκη κωδικοποίησης (Galetsi, Katsaliaki, & Kumar, 2023).

Οι πλατφόρμες Ασφάλειας Εφαρμογών για Κινητά και Πρόληψης Απάτης θα πρέπει να περιλαμβάνουν τα ακόλουθα στοιχεία ασφάλειας και πρόληψης απάτης για να βοηθήσουν τις εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές να συμμορφώνονται με τους κανονισμούς (Machado, Cunha, & Jorge Gouveia, 2023):

- Να δημιουργούν app hardening (ανθεκτικότητα) στην εφαρμογή υγειονομικής περίθαλψης για κινητά και να την προστατεύουν από προσπάθειες εντοπισμού σφαλμάτων, παραβίασης ή αναστροφής μηχανικής.
- Να έχουν την κατάλληλη κρυπτογράφηση, το οποίο αποτελεί το πιο σημαντικό στοιχείο στην πλατφόρμα που βοηθά τους οργανισμούς υγειονομικής περίθαλψης να συμμορφώνονται με τον GDPR και τον Νόμο για την Προστασία Δεδομένων. Με αυτή την ιδιότητα οι κατασκευαστές εφαρμογών μπορούν να προστατεύουν και να προστατεύουν όλες τις εγγραφές PHI και ePHI με κρυπτογράφηση δεδομένων, συμπεριλαμβανομένης της κρυπτογράφησης των δεδομένων ασθενών που είναι αποθηκευμένα σε συμβολοσειρές, πόρους και προτιμήσεις εφαρμογών.
- Να έχουν την αρμόζουσα obfuscation / συμπόλισμα η οποία κάνει μη ανιχνεύσιμο τον δυαδικό κώδικα, τις εγγενείς και μη εγγενείς βιβλιοθήκες και τον έλεγχο ροής και τη λογική της εφαρμογής.
- Να έχουν την πρόσφορη προστασία η οποία θα προφυλάσσει όλα τα δεδομένα της εφαρμογής mHealth κατά τη μεταφορά τους από επιθέσεις που βασίζονται σε δίκτυο όπως το MitM (Man-in-the-Middle attack) και θα διασφαλίζει την εγκυρότητα όλων των τελικών σημείων και τυχόν ενδιάμεσων συστημάτων μεταξύ των εφαρμογών υγειονομικής περίθαλψης για κινητά και του υποστηρικτικού τους συστήματος με ασφαλή καρφίτσωμα πιστοποιητικών, πιστοποιητικά πελατών για κινητά και πολλά άλλα. Επιπλέον να προστατεύει την εφαρμογή υγειονομικής περίθαλψης από τη λειτουργία σε μη ασφαλή περιβάλλοντα, όπως σε συσκευές Jailbroken/Rooted.

- Να παρέχουν προσθέτα FaceID, Touch ID και σύνθετους κωδικούς πρόσβασης σε εφαρμογές υγειονομικής περίθαλψης για κινητές συσκευές και θα συμβάλλουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης.

5.2 Data Protection By Default εφαρμογών Android υγείας από κρατικούς φορείς

Οι ψηφιακές τεχνολογίες, ιδίως οι κινητές συσκευές και οι βιομετρικές εφαρμογές, υιοθετούνται με καινοτόμους τρόπους για τη βελτίωση της αποτελεσματικότητας των κρατικών αντιδράσεων υγειονομικών προβλημάτων, όπως τον COVID-19.

Οι πληροφορίες και οι τάσεις που προκύπτουν είναι ανεκτίμητες για τις χώρες που επιδιώκουν να παρακολουθήσουν το ξέσπασμα του COVID-19, να προειδοποιήσουν τις ευάλωτες κοινότητες και να κατανοήσουν τον αντίκτυπο πολιτικών όπως η κοινωνική απόσταση και ο περιορισμός.

Η αποκάλυψη προσωπικών πληροφοριών μπορεί να επιτρέψει στο κοινό να εντοπίζει καλύτερα πιθανές λοιμώξεις από τον COVID-19 και να παρακολουθεί την εξάπλωση με την πάροδο του χρόνου. Ωστόσο, οι τρέχουσες ψηφιακές λύσεις για την παρακολούθηση και τον περιορισμό έχουν ποικίλες επιπτώσεις στην προστασία της ιδιωτικής ζωής και των δεδομένων (Adiyasa & Wirata, 2023).

Πλήρως διαφανείς και υπεύθυνες λύσεις για τη διατήρηση του απορρήτου θα πρέπει να ενσωματωθούν στο σχεδιασμό για να εξισορροπηθούν τα οφέλη και οι κίνδυνοι που σχετίζονται με τη συλλογή, τη διαδικασία και την κοινή χρήση προσωπικών δεδομένων. Τα δεδομένα θα πρέπει να διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο για την εξυπηρέτηση του συγκεκριμένου σκοπού για τον οποίο συλλέχθηκαν.

5.2.1 Συνεργασία χωρών με παρόχους τηλεπικοινωνιακών υπηρεσιών για την πρόσβαση σε δεδομένα γεωγραφικής θέσης παρακολούθησης μετακινήσεων πληθυσμού

Με αφορμή τον COVID-19, ο οποίος συνεχίζει να αφαιρεί ανθρώπινες ζωές και να επηρεάζει την παγκόσμια οικονομία, οι χώρες αναζητούν επειγόντως καινοτόμα νέα εργαλεία για την ενημέρωση της πολιτικής και την αντιμετώπιση της εκάστοτε υγειονομικής κρίσης. Ψηφιακές λύσεις που βασίζονται σε δεδομένα γεωγραφικού εντοπισμού αναδύονται για να βοηθήσουν τις αρχές να παρακολουθούν και να περιορίζουν την εξάπλωση του ιού. Ορισμένες τροφοδοτούνται από αρχεία δεδομένων κλήσεων κινητής τηλεφωνίας (call data records / CDR), δηλαδή δεδομένα που παράγονται από παρόχους τηλεπικοινωνιακών υπηρεσιών για τηλεφωνικές κλήσεις ή

άλλες τηλεπικοινωνιακές συναλλαγές, τα οποία παρέχουν πολύτιμες πληροφορίες για τις μετακινήσεις πληθυσμού. Καθώς οι φορείς εκμετάλλευσης δικτύων εξυπηρετούν σημαντικά τμήματα του πληθυσμού σε ολόκληρα έθνη, οι μετακινήσεις εκατομμυρίων ανθρώπων σε λεπτές χωρικές και χρονικές κλίμακες μπορούν να μετρηθούν σχεδόν σε πραγματικό χρόνο. Οι πληροφορίες και οι τάσεις που προκύπτουν είναι ανεκτίμητες για τις κυβερνήσεις που επιδιώκουν να παρακολουθήσουν το ξέσπασμα του COVID-19, προειδοποιούν τις ευάλωτες κοινότητες (Ahn & Park, 2022).

Οι πάροχοι τηλεπικοινωνιών σε ορισμένες χώρες του ΟΟΣΑ έχουν αρχίσει να μοιράζονται δεδομένα γεωγραφικής θέσης που βασίζονται σε CDR με τις κυβερνήσεις σε συγκεντρωτική, ανώνυμη μορφή. Για παράδειγμα:

1. Ο γερμανικός πάροχος τηλεπικοινωνιών Deutsche Telekom παρέχει ανώνυμα δεδομένα «ροών κίνησης» των χρηστών του στο Ινστιτούτο Robert-Koch, ένα ερευνητικό ινστιτούτο και κυβερνητική υπηρεσία που είναι αρμόδια για τον έλεγχο και την πρόληψη ασθενειών.
2. Το σχέδιο πέντε σημείων του Ομίλου Vodafone για την αντιμετώπιση του COVID-19 περιλαμβάνει την παροχή στις κυβερνήσεις μεγάλων ανωνυμοποιημένων συνόλων δεδομένων (όπως ένας συγκεντρωτικός και ανώνυμος χάρτης θερμότητας για την περιοχή της Λομβαρδίας) για να βοηθηθούν οι αρχές να κατανοήσουν καλύτερα τις μετακινήσεις πληθυσμού.
3. Η Ευρωπαϊκή Επιτροπή βρίσκεται επί του παρόντος σε επαφή με οκτώ ευρωπαίους τηλεπικοινωνιακούς φορείς για να λάβει από αυτούς ανώνυμα συγκεντρωτικά δεδομένα γεωγραφικής θέσης κινητής τηλεφωνίας, προκειμένου να συντονίσει τα μέτρα παρακολούθησης της εξάπλωσης του COVID-19. Για να αντιμετωπιστούν οι ανησυχίες περί απορρήτου, τα δεδομένα θα διαγραφούν μόλις τελειώσει η κρίση.

5.2.2 Η εμπειρία από τις εφαρμογές ιχνηλάτησης COVID-19 ασθενών

Οι εφαρμογές συμβουλών υγείας για κινητές συσκευές αποτελούσαν ήδη σημαντικό μέρος του οικοσυστήματος υγείας για κινητά και έχουν αποδειχθεί αποτελεσματικές για σκοπούς πρόληψης, έγκαιρης διάγνωσης (π.χ. έλεγχοι συμπτωμάτων) και για τη σύνδεση των χρηστών με τοπικές υπηρεσίες υγείας και μονάδες έκτακτης ανάγκης. Τώρα, εμφανίζονται νέες εφαρμογές που απευθύνονται στους καταναλωτές με στόχο την παρακολούθηση του COVID-19. Αυτές οι εφαρμογές αναπτύσσονται όλο και περισσότερο ως ανοιχτού κώδικα και είναι προϊόν συνεργασιών τεχνολογικών εταιρειών, ακαδημαϊκού κόσμου, κλινικών ιατρών και δημόσιων αρχών, οι οποίες είναι

τελικά υπεύθυνες για τη χρηματοδότηση, την περαιτέρω ανάπτυξη και την εφαρμογή τους. Αν και δεν συλλαμβάνετε απαραίτητα όλο τον πληθυσμό (π.χ. ηλικιωμένους που μπορεί να μην έχουν ή να είναι ικανοί στη χρήση smartphone), ούτε χωρίς κάποιο λάθος (π.χ. όταν δεν μπορούν να διακρίνουν άτομα του ίδιου νοικοκυριού και εκείνων στις γύρω κατοικίες), αυτές οι εφαρμογές παρέχουν ένα άλλο εργαλείο στις κυβερνήσεις για την παρακολούθηση και τον περιορισμό του ιού. Μεταξύ των πιο αναφερόμενων είναι:

- TraceTogether: Αναπτύχθηκε από την Κυβερνητική Υπηρεσία Τεχνολογίας της Σιγκαπούρης (GovTech) σε συνεργασία με το Υπουργείο Υγείας, χρησιμοποιώντας Bluetooth, αυτή η εφαρμογή παρακολουθεί άτομα που έχουν εκτεθεί στον ιό. Αυτές οι πληροφορίες χρησιμοποιούνται για τον εντοπισμό στενών επαφών με βάση την εγγύτητα και τη διάρκεια μιας συνάντησης μεταξύ δύο χρηστών. Στη συνέχεια ειδοποιεί όσους έρχονται σε επαφή με κάποιον που έχει βγει θετικός ή διατρέχει υψηλό κίνδυνο να μεταφέρει τον κοροναϊό. Μόλις επιβεβαιωθεί ή υποψιαστεί ότι ένα άτομο έχει μολυνθεί, μπορεί να επιλέξει να επιτρέψει στα νοσοκομεία, το Υπουργείο Υγείας και τρίτα μέρη να έχουν πρόσβαση σε δεδομένα στην εφαρμογή για να βοηθήσουν στον εντοπισμό στενών επαφών. Η Σιγκαπούρη σχεδιάζει να δημιουργήσει το υποκείμενο πρωτόκολλο διατήρησης της ιδιωτικής ζωής για την ανταλλαγή δεδομένων που το TraceTogether βασίζεται σε ανοιχτό κώδικα (TraceTogether, 2020).
- Pan-European Privacy-Preserving Proximity Tracing (Πανευρωπαϊκός εντοπισμός εγγύτητας με προστασία της ιδιωτικής ζωής): Πάνω από 130 επιστήμονες, τεχνολόγοι και εμπειρογνώμονες από οκτώ ευρωπαϊκές χώρες – συμπεριλαμβανομένης της Γαλλίας, της Γερμανίας και της Ιταλίας– συμμετείχαν σε μια μη κερδοσκοπική πρωτοβουλία που ανέπτυξε μια εφαρμογή ανοιχτού κώδικα που αναλύει τα σήματα Bluetooth μεταξύ κινητών τηλεφώνων εντοπισμός χρηστών που βρίσκονταν σε κοντινή απόσταση μεταξύ τους. Η εφαρμογή αποθηκεύει προσωρινά αυτά τα κρυπτογραφημένα δεδομένα τοπικά και εάν οι χρήστες αργότερα βγουν θετικοί στον COVID-19, μπορεί να ειδοποιήσει οποιονδήποτε βρισκόταν γύρω από το μολυσμένο άτομο τις προηγούμενες ημέρες, διατηρώντας παράλληλα προστατευμένη την ταυτότητα όλων των χρηστών (PEPP-PT/mhealth-hub, 2020).
- Korea's Tracking App / Εφαρμογή παρακολούθησης της Κορέας: Χρηματοδοτείται από την κυβέρνηση της Κορέας, η εφαρμογή ασφαλείας αυτο-καραντίνας που χρησιμοποιείται από καθορισμένες δημόσιες αρχές για την παροχή πληροφοριών

σχετικά με τον COVID-19, συμπεριλαμβανομένων των κατευθυντήριων γραμμών καραντίνας και για την πρόληψη πιθανών παραβιάσεων των εντολών αυτό-καραντίνας. Η εφαρμογή μπορεί επίσης να χρησιμοποιηθεί για αυτοέλεγχο και εθελοντική αναφορά στις αρχές υγειονομικής περίθαλψης. Τα δεδομένα που συλλέγονται δεν κοινοποιούνται σε τρίτους.

- C-19 COVID Symptom Tracker / Παρακολούθηση συμπτωμάτων COVID C-19: Ο στόχος αυτής της εφαρμογής αναπτύχθηκε στο Ηνωμένο Βασίλειο ως συνεργασία μεταξύ γιατρών και επιστημόνων στο King's College του Λονδίνου, μιας εταιρείας επιστήμης δεδομένων υγείας και του Εθνικού Ινστιτούτου Ερευνητικού Κέντρου Υγείας στο Guy's and St Thomas'. Τα νοσοκομεία πρόκειται να επιβραδύνουν το ξέσπασμα του COVID-19 βοηθώντας τους ερευνητές να εντοπίσουν: i) πόσο γρήγορα εξαπλώνεται ο ιός σε διάφορες περιοχές. ii) περιοχές υψηλού κινδύνου στο Ηνωμένο Βασίλειο και iii) ποιος κινδυνεύει περισσότερο, κατανοώντας καλύτερα τα συμπτώματα που σχετίζονται με υποκείμενες παθήσεις υγείας. Σύμφωνα με τους ερευνητές, τα δεδομένα από τη μελέτη μπορούν να αποκαλύψουν βασικές πληροφορίες σχετικά με τα συμπτώματα και την πρόοδο της λοίμωξης σε διαφορετικούς ανθρώπους. Μπορεί επίσης να βοηθήσει τους ερευνητές να κατανοήσουν γιατί ορισμένα άτομα αναπτύσσουν πιο σοβαρά ή θανατηφόρα συμπτώματα ενώ άλλα έχουν μόνο ήπια συμπτώματα λόγω του COVID-19.

- Επιπλέον, η Apple και η Google θα κυκλοφορήσουν επίσης API που επιτρέπουν τη διαλειτουργικότητα μεταξύ συσκευών Android και iOS χρησιμοποιώντας εφαρμογές από αρχές δημόσιας υγείας. Οι χρήστες θα μπορούν να κάνουν λήψη αυτών των εφαρμογών μέσω των αντίστοιχων καταστημάτων εφαρμογών τους. Οι δύο εταιρείες θα συνεργαστούν επίσης για να ενεργοποιήσουν μια ευρύτερη πλατφόρμα ανίχνευσης επαφών που βασίζεται σε Bluetooth, ενσωματώνοντας αυτή τη λειτουργικότητα στις υποκείμενες πλατφόρμες. Αυτή η λύση θα επέτρεπε σε περισσότερα άτομα να συμμετέχουν σε περίπτωση που αποφασίσουν να επιλέξουν τη συμμετοχή και θα μπορούσε να βελτιώσει την αλληλεπίδραση με ένα ευρύτερο οικοσύστημα εφαρμογών και κρατικές αρχές υγείας.

5.2.3 Ενσωμάτωση βαθμών προστασίας απορρήτου και δεδομένων σε εφαρμογές παρακολούθησης

Η χρήση εφαρμογών συλλογής δεδομένων γεωγραφικής τοποθεσίας μπορεί να επιτρέψει την κοινή χρήση δεδομένων με ρητή, ενσωματωμένη προστασία απορρήτου και δεδομένων και να επιτρέψει στους χρήστες να δώσουν τη ρητή, ενημερωμένη

συγκατάθεσή τους για τη συλλογή και την κοινή χρήση των προσωπικών τους δεδομένων (υποθέτοντας ότι η χρήση της εφαρμογής είναι δεν είναι υποχρεωτικό). Για παράδειγμα, η εφαρμογή TraceTogether της Σιγκαπούρης διαθέτει μια σειρά από εγγυήσεις απορρήτου, συμπεριλαμβανομένου ότι δεν συλλέγει ή χρησιμοποιεί δεδομένα γεωγραφικής τοποθεσίας και ότι τα αρχεία καταγραφής δεδομένων αποθηκεύονται σε κρυπτογραφημένη μορφή. Για την προστασία του απορρήτου των χρηστών της, η Πανευρωπαϊκή εφαρμογή κρυπτογραφεί δεδομένα και ανωνυμοποιεί τις προσωπικές πληροφορίες. Επιπλέον, καθώς δύο τηλέφωνα δεν ανταλλάσσουν ποτέ δεδομένα απευθείας και τα ψευδώνυμα των χρηστών αλλάζουν συχνά, είναι σχεδόν αδύνατο να αποκαλυφθεί η ταυτότητα των χρηστών (Li, και συν., 2023).

Ωστόσο, το εύρος των προσωπικών δεδομένων που συλλέγουν, επεξεργάζονται και μοιράζονται αυτές οι εφαρμογές μπορεί να είναι πολύ ευρύ και δύσκολο να το κατανοήσουν οι χρήστες. Σε πολλές περιπτώσεις, οι εφαρμογές συνεχίζουν να εκτελούνται στο παρασκήνιο ακόμα και όταν η συσκευή δεν χρησιμοποιείται. Ορισμένες εφαρμογές μπορούν επίσης να ανταλλάσσουν πληροφορίες με άλλες εφαρμογές μέσω διεπαφών προγραμματισμού εφαρμογών (application programming interfaces / API), δημιουργώντας πιο λεπτομερείς πληροφορίες. Ενώ ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) επαίνεσε τα εκτεταμένα μέτρα εντοπισμού της Κορέας, ορισμένες χρήσεις από τις καθορισμένες τοπικές αρχές των δεδομένων που συλλέγονται μέσω του Συστήματος Υποστήριξης Επιδημιολογικής Έρευνας σχετικά με τις μετακινήσεις ατόμων με επιβεβαιωμένα κρούσματα έχουν εγείρει ανησυχίες για την προστασία της ιδιωτικής ζωής (OECD/Tracking and tracing COVID, 2020).

5.2.4 Η αξιοποίηση βιομετρικών δεδομένων προσθέτει οφέλη και προκλήσεις

Η αναγνώριση προσώπου αποτέλεσε ένα από τα πιο συχνά χρησιμοποιούμενα βιομετρικά στοιχεία σε πολλές χώρες για την παρακολούθηση της εξάπλωσης του COVID-19. Η αναγνώριση προσώπου επέτρεψε στις αρχές να μειώσουν τη χρήση τεχνολογιών αναγνώρισης που απαιτούν φυσική επαφή (όπως σαρώσεις ίριδας και δακτυλικά αποτυπώματα). Μπορεί επίσης να συνδυαστεί με άλλες τεχνολογίες, συμπεριλαμβανομένης της θερμικής απεικόνισης που ενισχύεται από την τεχνητή νοημοσύνη, για την καλύτερη παρακολούθηση πολιτών που ενδέχεται να είναι θετικοί στον COVID-19 (OECD/Tracking and tracing COVID, 2020).

Στην Πολωνία, η κυβέρνηση κυκλοφόρησε μια βιομετρική εφαρμογή smartphone για να επιβεβαιώσει ότι τα άτομα που έχουν μολυνθεί από τον COVID-19 παραμένουν σε

καραντίνα. Στη Λαϊκή Δημοκρατία της Κίνας, η αναγνώριση προσώπου έχει χρησιμοποιηθεί για την αποτροπή ταξιδιών πολιτών που μπορεί να έχουν μολυνθεί από τον COVID-19. Επιπλέον, εταιρείες στην Κίνα έχουν αναπτύξει μια τεχνολογία που θα μπορούσε να επιτρέψει στην κυβέρνηση να εντοπίζει με επιτυχία άτομα ακόμα και όταν φορούν μάσκες. Στη Ρωσική Ομοσπονδία, τα συστήματα αναγνώρισης προσώπου χρησιμοποιούνται για την παρακολούθηση ατόμων που δεν τηρούν την υποχρεωτική καραντίνα.

Ωστόσο, η χρήση βιομετρικών στοιχείων (συμπεριλαμβανομένης της αναγνώρισης προσώπου) ως απάντηση στον COVID-19 εγείρει μια σειρά ανησυχιών σχετικά με το απόρρητο και την ασφάλεια, ιδιαίτερα όταν αυτές οι τεχνολογίες χρησιμοποιούνται ελλείψει συγκεκριμένης καθοδήγησης ή πλήρως ενημερωμένης και ρητής συναίνεσης. Τα άτομα μπορεί επίσης να αντιμετωπίζουν προβλήματα κατά την άσκηση ενός ευρέος φάσματος θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένου του δικαιώματος πρόσβασης στα προσωπικά τους δεδομένα, του δικαιώματος διαγραφής και του δικαιώματος ενημέρωσης σχετικά με τους σκοπούς της επεξεργασίας και με ποιους κοινοποιούνται αυτά τα δεδομένα. Τα συστήματα αναγνώρισης προσώπου μπορεί επίσης να έχουν εγγενή τεχνολογική προκατάληψη, π.χ. όταν βασίζονται σε φυλετική ή εθνική καταγωγή (OECD/Tracking and tracing COVID, 2020). Εξάλλου, η αυτοματοποιημένη αναγνώριση προσώπου αποτελεί επεξεργασία ευαίσθητων προσωπικών δεδομένων σύμφωνα με τον GDPR, το οποίο συνεπάγεται απαίτηση για πρόσθετες διασφαλίσεις προκειμένου η επεξεργασία τους να είναι νόμιμη.

5.2.5 Το απόρρητο ανά σχέδιο/ Privacy-by-design στην αντιμετώπιση κινδύνων

Το Privacy-by-design[11] επιδιώκει να προσφέρει τον μέγιστο βαθμό απορρήτου διασφαλίζοντας ότι οι προστασίες προσωπικών δεδομένων είναι ενσωματωμένες στο σύστημα, από προεπιλογή. Το Privacy-by-design μπορεί, για παράδειγμα, να περιλαμβάνει τη χρήση συγκεντρωτικών, ανωνυμοποιημένων ή ψευδώνυμων

[11] Τα «Privacy by Design / Απόρρητο κατά σχεδιασμό» και «Privacy by Default / Απόρρητο από προεπιλογή» έχουν συζητηθεί συχνά θέματα σχετικά με την προστασία δεδομένων. Οι πρώτες σκέψεις του «Privacy by Design» εκφράστηκαν τη δεκαετία του 1970 και ενσωματώθηκαν τη δεκαετία του 1990 στην οδηγία RL 95/46/EC για την προστασία δεδομένων. Σύμφωνα με την αιτιολογική σκέψη 46 της παρούσας οδηγίας, τεχνικά και οργανωτικά μέτρα (TOM) πρέπει να λαμβάνονται ήδη κατά τον σχεδιασμό ενός συστήματος επεξεργασίας για την προστασία της ασφάλειας δεδομένων.

δεδομένων για την παροχή πρόσθετης προστασίας του απορρήτου ή τη διαγραφή δεδομένων μόλις εκπληρωθεί ο σκοπός τους (Privacy by Design, 2016).

Για παράδειγμα, η εφαρμογή COVID-19 που αναπτύχθηκε από το Νορβηγικό Ινστιτούτο Δημόσιας Υγείας έχει σχεδιαστεί για να αποθηκεύει δεδομένα τοποθεσίας μόνο για 30 ημέρες. Η χρήση πρόσθετων λύσεων ενίσχυσης του απορρήτου (όπως ομομορφική κρυπτογράφηση) μπορεί να παρέχει πρόσθετη ασφάλεια, όπως και η χρήση sandbox δεδομένων, μέσω των οποίων η πρόσβαση σε εξαιρετικά ευαίσθητα (προσωπικά) δεδομένα παρέχεται μόνο σε περιορισμένο ψηφιακό ή/και φυσικό περιβάλλον σε αξιόπιστους χρήστες. Ένα παράδειγμα της τελευταίας είναι η Flowminder, η οποία συνεργάστηκε με εταιρείες τηλεπικοινωνιών κατά την έξαρση του Έμπολα το 2014-16 για να παρέχει στους επιδημιολόγους ασφαλή πρόσβαση σε μη αναγνωρισμένα δεδομένα γεωεντοπισμού χαμηλής ανάλυσης. Η Flowminder χρησιμοποιεί παρόμοια στρατηγική για να συμβάλει στην αντιμετώπιση της κρίσης του COVID-19.

5.2.6 Βασικές συστάσεις

Οι ψηφιακές τεχνολογίες παρέχουν ισχυρά εργαλεία για τις κυβερνήσεις στον αγώνα τους για τον έλεγχο της πανδημίας COVID-19, αλλά πρέπει να αναγνωριστούν οι επιπτώσεις τους στο απόρρητο και στην προστασία των δεδομένων. Οι εφαρμογές ανίχνευσης επαφών θα πρέπει να υλοποιούνται με πλήρη διαφάνεια, σε συνεννόηση με τους κύριους ενδιαφερόμενους φορείς, ισχυρές προστασίες απορρήτου ανά σχεδιασμό και μέσω έργων ανοιχτού κώδικα (όπου χρειάζεται). Οι κυβερνήσεις θα πρέπει να εξετάσουν:

- Η νομική βάση της χρήσης αυτών των τεχνολογιών, η οποία ποικίλλει ανάλογα με τον τύπο των δεδομένων που συλλέγονται (π.χ. προσωπικά, ευαίσθητα, ψευδώνυμα, ανώνυμα, συγκεντρωτικά, δομημένα ή μη).
- Εάν η χρήση αυτών των τεχνολογιών και η επακόλουθη συλλογή δεδομένων είναι αναλογική και εξετάστε τον τρόπο αποθήκευσης, επεξεργασίας, κοινής χρήσης και με ποιον τα δεδομένα (συμπεριλαμβανομένων των πρωτοκόλλων ασφάλειας και απορρήτου που εφαρμόζονται ανά σχεδιασμό).
- Η ποιότητα των δεδομένων που συλλέγονται και αν είναι κατάλληλα για τον σκοπό.
- Εάν το κοινό είναι καλά ενημερωμένο και οι προσεγγίσεις που υιοθετούνται εφαρμόζονται με πλήρη διαφάνεια και υπευθυνότητα.

- Η χρονική περίοδος εντός της οποίας μπορούν να χρησιμοποιηθούν πιο επεμβατικές τεχνολογίες που συλλέγουν προσωπικά δεδομένα για την καταπολέμηση της κρίσης. Τα δεδομένα θα πρέπει να διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο για την εξυπηρέτηση του συγκεκριμένου σκοπού για τον οποίο συλλέχθηκαν.

Κεφάλαιο 6
Εφαρμογές Android από δημόσιους φορείς – Η περίπτωση των εφαρμογών υγείας

Στο παρόν κεφάλαιο παρουσιάζονται διάφορες κρατικές εφαρμογές υγείας Android ανά τον κόσμο (Coronapas της Δανίας, Passe Covid της Πορτογαλίας, CovPass της Γερμανίας, CovScan Cyprus και CovPass Cyprus της Κυπριακής Κυβέρνησης, Covid Free GR και MyHealth της Ελληνικής Δημοκρατίας, COVID Alert NJ από το Υπουργείο Υγείας του Νιου Τζέρσεϋ (DOH), WHO Info και OpenWHO του Παγκόσμιου Οργανισμού Υγείας / ΠΟΥ). Θα καταγραφούν οι βαθμολογίες, οι αξιολογήσεις και η ασφάλεια δεδομένων από την πλατφόρμα Google Play και τέλος θα πραγματοποιηθεί έλεγχος με το διαδικτυακό εργαλείο Exodus Privacy.

Οι εφαρμογές επελέγησαν με γνώμονα τη δημοφιλία τους, όπως αποτυπώνεται στο Google App Store, αλλά και με την κάλυψη διαφορετικών γεωγραφικών ηπείρων, όπου υπάρχει διαφορετικό νομοθετικό πλαίσιο στην κάθε μία. Επίσης εξετάστηκαν χαρακτηριστικές εφαρμογές αυτής της κατηγορίας που προσφέρονται σε Κύπρο και Ελλάδα.

Σημειώνεται ότι, λόγω της πρόσφατης πανδημίας του COVID-19, οι περισσότερες εφαρμογές στον τομέα που εξετάζει η παρούσα διατριβή αφορούν είτε την περίπτωση ελέγχου πιστοποιητικών COVID-19 είτε την περίπτωση ιχνηλάτησης κρουσμάτων. Παρά το γεγονός ότι πλέον δεν γίνεται χρήση αυτών των εφαρμογών, έχει εξαιρετικό ενδιαφέρον να διαπιστωθεί σε τι βαθμό υπήρξαν εγγυήσεις, ως προς την προστασία προσωπικών δεδομένων, από τους αρμόδιους κρατικούς φορείς οι οποίοι διέθεσαν τέτοιες εφαρμογές.

6.1 Coronapas

Η εφαρμογή Coronapas - Τεστ COVID-19, αποτελεί Android εφαρμογή υγείας από το δημόσιο φορέα υγείας της Δανίας. Η Coronapas πληροί τις απαιτήσεις για το ψηφιακό πιστοποιητικό covid της ΕΕ. Ο εκάστοτε χρήστης μπορεί να παραλάβει το διαβατήριό του για το κορωναϊό για το τεστ COVID-19 εάν έχει βγει αρνητικός για COVID-19 και το τεστ δεν είναι παλαιότερο των επτά ημερών. Το Statens Serum Institut και η Region Nordjylland είναι η αρμόδια αρχή δεδομένων για το τεστ Coronapas - COVID-19 (Coronapas - COVID-19 test, 2020).

Εικόνα 6.1: Όνομα και λογότυπο της εφαρμογής Coronapas - Τεστ COVID-19.

Ο εκάστοτε χρήστης μπορεί να συνδεθεί με το NemID και να δει τα δεδομένα υγείας που έχει καταχωρίσει η κυβέρνηση της Δανίας για τον ίδιο. Στο μητρώο υγείας του, θα βρει τις πιο πρόσφατες πληροφορίες που έχουν καταχωρηθεί για τον χρήστη σχετικά με θεραπείες, φάρμακα, αλλεργίες σε φάρμακα, εργαστηριακά αποτελέσματα κ.λπ. Έχει επίσης τη δυνατότητα να καταχωρίσει τη θέση του σχετικά με τη δωρεά οργάνων ή να δημιουργήσει μια διαθήκη θεραπείας. Επιπλέον στο αρχείο υγείας, μπορεί να δει δεδομένα υγείας που έχει καταχωρίσει η υπηρεσία υγείας για τον χρήστη, μεταξύ άλλων, τον ιατρικό νοσοκομειακό φάκελο, αποτελέσματα εξετάσεων, τις ιατρικές παραπομπές, την κάρτα φαρμάκων και μια συνολική επισκόπηση του πότε έχει επισκεφτεί γιατρό, οδοντίατρο, φυσιοθεραπευτή κ.λπ. (Coronapas - COVID-19 test, 2020).

6.1.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Coronapas από τους 9190 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,6/5 (εικόνα 6.2).

Εικόνα 6.2: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Coronapas,

από τους 9190 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.1.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Για να υφίστανται τα παραπάνω της εφαρμογή Coronapas χρειάζεται «Δήλωση συγκατάθεσης». Δηλαδή ο εκάστοτε χρήστης πρέπει να συναινέσει ώστε τα προσωπικά του δεδομένα υγείας να εμφανίζονται για τον ίδιο στο sundhed.dk, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και τον Νόμο για την Προστασία Δεδομένων.

Η ασφάλεια δεδομένων ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του εκατοστέ χρήστη. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (Coronapas, 2020):.

- Η εφαρμογή Coronapas ενδέχεται να κοινοποιεί τύπους δεδομένων σε τρίτα μέρη (όπως: πληροφορίες και απόδοση εφαρμογής και αναγνωριστικά συσκευής ή άλλα αναγνωριστικά).
- Η εφαρμογή Coronapas ενδέχεται να συλλέγει τύπους δεδομένων (όπως: προσωπικά στοιχεία, Υγεία και φυσική κατάσταση).
- Τα δεδομένα κρυπτογραφούνται κατά τη μεταφορά.
- Δύναται αίτηση διαγραφής δεδομένων.

6.1.3 Έλεγχος της εφαρμογή Coronapas με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή Coronapas με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.3) παρατηρείται ότι δεν έχει ιχνηλάτες (trackers). Όσον αφορά τις άδειες / δικαιώματα έχει 9 και είναι οι εξής:

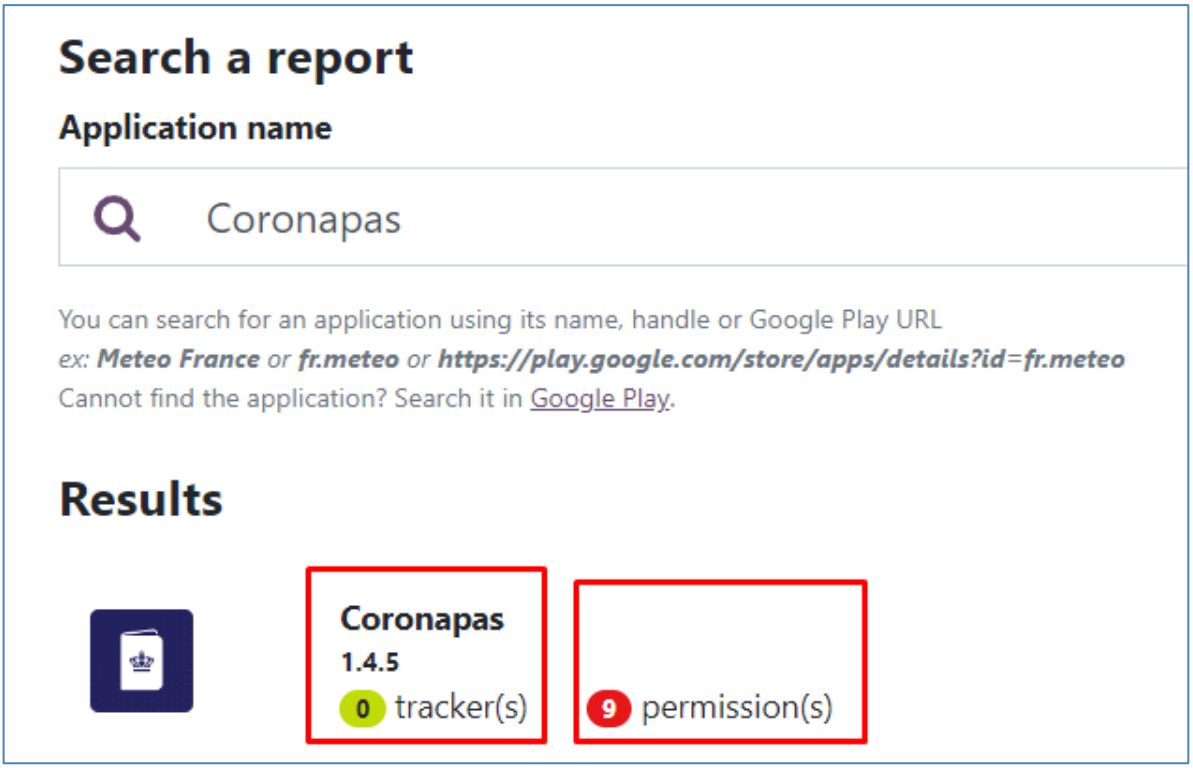
1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Flashlight
4. Internet: για πλήρη πρόσβαση στο δίκτυο
5. Use_Biometric: χρησιμοποιεί βιομετρικό υλικό
6. Use_Fingerprint: χρήση υλικού δακτυλικών αποτυπωμάτων
7. Vibrate: έλεγχος των κραδασμών
8. Wake_Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε αναστολή

9. Decode

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Coronapas, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας.

Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Βεβαίως στην ιστοσελίδα: https://www.coronapass.org/privacy-policy/ όπου καταγράφονται τα privacy policy της εφαρμογής Coronapas δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής Coronapas: «*Η πολιτική απορρήτου μας βασίζεται στους όρους που χρησιμοποιεί ο Ευρωπαίος νομοθέτης για την υιοθέτηση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR)*» (coronapass/privacy policy, 2021).



Εικόνα 6.3: Έλεγχος της εφαρμογή Coronapas με το διαδικτυακό εργαλείο Exodus Privacy.

6.2 Passe Covid

Η εφαρμογή Passe Covid αποτελεί Android εφαρμογή υγείας από το δημόσιο φορέα υγείας της Πορτογαλίας μπορεί να μεταφορτωθεί και να χρησιμοποιηθεί από όλους,

δηλαδή αερομεταφορείς, διοργανωτές πολιτιστικών, εταιρικών, αθλητικών και οικογενειακών εκδηλώσεων (όπως γάμοι και βαπτίσεις), έτσι ώστε να υπάρχει η δυνατότητα της ομαλότητας των ημερών της πανδημίας Covid, με όλη την ασφάλεια.

Εικόνα 6.4: Όνομα και λογότυπο εφαρμογή Passe Covid.

Μπορεί να χρησιμοποιηθεί από οντότητες που πρέπει να επικυρώσουν τα ψηφιακά πιστοποιητικά Covid της ΕΕ, που εκδίδονται από όλα τα κράτη μέλη της ΕΕ, την Ισλανδία, το Λιχτενστάιν, τη Νορβηγία και την Ελβετία.

Η εφαρμογή επικυρώνει την αυθεντικότητα του ψηφιακού πιστοποιητικού Covid της ΕΕ και τη συμμόρφωση με τα πορτογαλικά κριτήρια επικύρωσης που ορίζονται από το DGS (νομοθετικό διάταγμα αριθ. 54-A / 2021) (Passe Covid, 2021).

6.2.1 Τρόποι χρήσης

Στρέφεται η κάμερα του τηλεφώνου του εκάστοτε χρήστη για να σαρώσει τον κωδικό QR του εμφανιζόμενου πιστοποιητικού. Το πιστοποιητικό μπορεί να παρουσιαστεί σε έντυπη ή ψηφιακή μορφή. Η εφαρμογή θα επαληθεύσει αυτόματα το πιστοποιητικό.

Το αποτέλεσμα με πράσινο σήμα σημαίνει ότι το πιστοποιητικό επικυρώθηκε με επιτυχία.

Το αποτέλεσμα με ένα κόκκινο σήμα σημαίνει ότι το πιστοποιητικό δεν είναι έγκυρο (η επικύρωση περιλαμβάνει τον έλεγχο της γνησιότητας του πιστοποιητικού και τη συμμόρφωση με τους υγειονομικούς κανόνες της χώρας).

Αυτή η εφαρμογή δεν εγγυάται την ασφάλεια του κατόχου του ψηφιακού πιστοποιητικού COVID σε σχέση με το COVID-19, ούτε την ταυτότητά του, που χρησιμεύει μόνο για την επικύρωση της γνησιότητας του πιστοποιητικού.

Η παρουσίαση του Ψηφιακού Πιστοποιητικού COVID δεν χρησιμεύει ως μορφή αναγνώρισης του κατόχου, χωρίς πάντοτε να παρουσιάζεται ένα έγκυρο και νόμιμο επίσημο έγγραφο αναγνώρισης (Passe Covid, 2021).

6.2.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια της εφαρμογής Passe Covid ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του εκάστοτε χρήστη. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του χρήστη. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (Passe Covid, 2021).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Η εφαρμογή δεν αποθηκεύει κανένα τύπο δεδομένων.

6.2.3 Έλεγχος της εφαρμογή Passe Covid με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή Passe Covid με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.5) παρατηρείται ότι έχει βρεθεί 1 ιχνηλάτης (trackers) με υπογραφή κώδικα στην εφαρμογή: Conversant. Περιλαμβάνει Greystripe, εξατομικευμένο διαφημιστικό μάρκετινγκ, σε πλατφόρμα διαφήμισης για κινητά που αποκτήθηκε από την Conversant[12].

Όσον αφορά τις άδειες / δικαιώματα έχει 4 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Flashlight
4. Internet: για πλήρη πρόσβαση στο δίκτυο

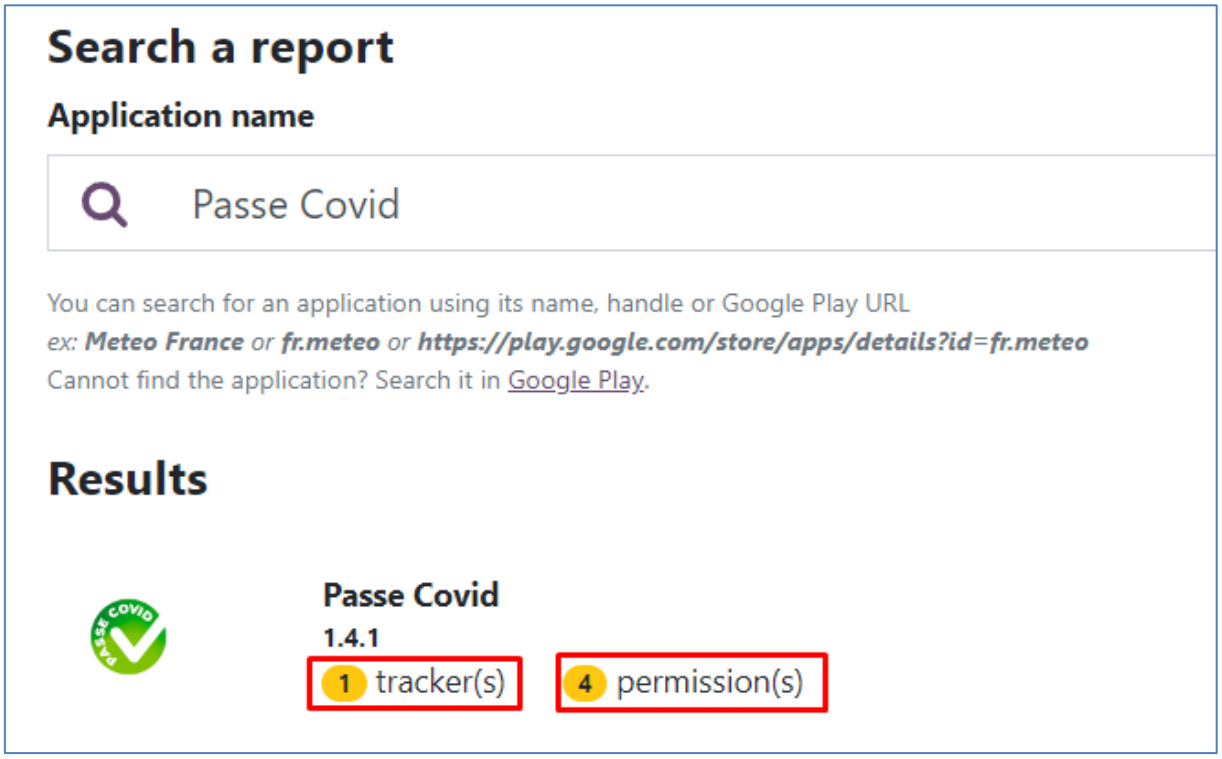
Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Passe Covid, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας.

Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

[12] Κανόνες ανίχνευσης:

- Κανόνας ανίχνευσης κώδικα: com.conversantmedia | com.greystripe.android.
- Κανόνας ανίχνευσης δικτύου: conversantmedia\.com

Ασφαλώς στην ιστοσελίδα: https://covidpass.eu/en/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής Passe Covid δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions) και ο ιχνηλάτης (trackers). Σύμφωνα με το τμήμα privacy policy της εφαρμογής Passe Covid: «*Τα δεδομένα σας δεν αποθηκεύονται πέρα από την ενεργή περίοδο λειτουργίας του προγράμματος περιήγησης και ο ιστότοπος δεν χρησιμοποιεί cookies.…Δεν αποστέλλονται δεδομένα σε τρίτους*)» (Passe Covid / privacy policy, 2021).



Εικόνα 6.5: Έλεγχος της εφαρμογή Passe Covid με το διαδικτυακό εργαλείο Exodus Privacy.

6.3 CovPass

Το Ινστιτούτο Robert Koch (RKI) ως κεντρικό ομοσπονδιακό ίδρυμα στον τομέα της δημόσιας υγείας και ως εθνικό ινστιτούτο δημόσιας υγείας δημοσιεύει την εφαρμογή CovPass για τη γερμανική ομοσπονδιακή κυβέρνηση. Με την εφαρμογή αυτή, τα ψηφιακά πιστοποιητικά COVID της ΕΕ μπορούν να αποθηκευτούν απευθείας στο smartphone του εκάστοτε χρήστη. Όσοι τα χρησιμοποιούν μπορούν να αποδείξουν γρήγορα και αξιόπιστα την εμβολιαστική τους προστασία ή ανάρρωση. Η εφαρμογή μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση των ψηφιακών πιστοποιητικών COVID της ΕΕ από άλλα άτομα (π.χ. μέλη της οικογένειας) στα smartphone τους. Οι

χρήστες της εφαρμογής αποφασίζουν πότε και σε ποιον θα εμφανίσουν τις πληροφορίες και τα δεδομένα τους.

Εικόνα 6.6: Όνομα και λογότυπο της εφαρμογής CovPass.

6.3.1 Τρόποι χρήσης

Η απόδειξη των εμβολιασμών και η ανάρρωση από μόλυνση για COVID είναι η κεντρική λειτουργία της εφαρμογής CovPass. Κάθε φορά που οι χρήστες αποδεικνύουν την κατάστασή τους, μόνο οι πληροφορίες και τα δεδομένα που είναι απαραίτητα για την επαλήθευση εμφανίζονται μέσω κωδικού QR (CovPass, 2021).

Ο κωδικός QR παρέχει πληροφορίες σχετικά με την εγκυρότητα ενός πιστοποιητικού εμβολιασμού ή ανάρρωσης. Το όνομα και η ημερομηνία γέννησης εμφανίζονται επίσης κατά τη διάρκεια ενός ελέγχου για σαφή αναγνώριση.

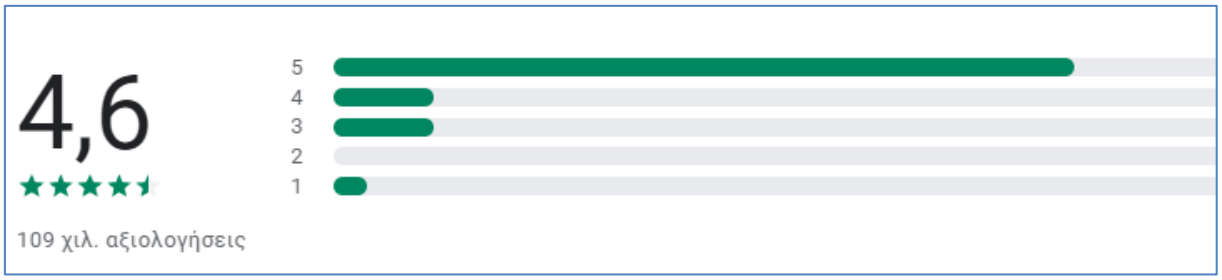
Οι εμβολιασμοί για COVID μπορούν να πιστοποιηθούν με το ψηφιακό πιστοποιητικό εμβολιασμού COVID της ΕΕ κατόπιν αιτήματος. Το πιστοποιητικό εκδίδεται από το ιατρικό προσωπικό μετά τον εμβολιασμό. Περιέχει έναν κωδικό QR που μπορεί να σαρωθεί με την εφαρμογή CovPass. Για να γίνει αυτό, κρατάται η κάμερα του smartphone πάνω από τον κωδικό QR. Στη συνέχεια, όλες οι πληροφορίες στο πιστοποιητικό φορτώνονται απευθείας στο smartphone και ο τρέχων κωδικός QR εμφανίζεται στην οθόνη έναρξης της εφαρμογής. Αυτό μπορεί τώρα να εμφανιστεί με την εφαρμογή CovPass, εάν απαιτείται.

Οι ανακτήσεις από μόλυνση από COVID είναι πιστοποιημένες με το ψηφιακό πιστοποιητικό αποκατάστασης COVID από την ΕΕ. Θα ληφθεί από τον εκάστοτε χρήστη το πιστοποιητικό αποκατάστασης από τον γενικό ιατρό του ή από το τοπικό τμήμα υγείας αφού έχει ξεπεράσει την ασθένεια κορονοϊού. Περιέχει έναν κωδικό QR που μπορεί να σαρωθεί με την εφαρμογή. Το πιστοποιητικό ανάκτησης τεκμηριώνεται στη συνέχεια στο smartphone.

Τα ψηφιακά πιστοποιητικά COVID από την ΕΕ από άλλα άτομα (π.χ. μέλη της οικογένειας) μπορούν επίσης να διαχειριστούν στο smartphone (CovPass, 2021).

6.3.2 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass από τους 109000 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,6/5 (εικόνα 6.7) (CovPass, 2021).



Εικόνα 6.7: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass,

από τους 109000 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.3.3 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Τα δεδομένα του ψηφιακού πιστοποιητικού COVID της ΕΕ αποθηκεύονται τοπικά στο smartphone. Μόνο οι χρήστες αποφασίζουν πότε και σε ποιον θα εμφανίσουν τις πληροφορίες και τα δεδομένα.

Η ασφάλεια ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του εκάστοτε χρήστη. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου. Η προστασία δεδομένων διατηρείται καθ' όλη τη διάρκεια της χρήσης (CovPass, 2021).

- **Χωρίς εγγραφή**: Δεν απαιτείται εγγραφή με διεύθυνση e-mail.
- **Αποθήκευση τοπικών δεδομένων**: Τα πλήρη δεδομένα αποθηκεύονται μόνο στο smartphone του εκάστοτε χρήστη.
- **Οικονομία δεδομένων**: Ο κωδικός QR εμφανίζεται με τον ελάχιστο όγκο δεδομένων που έχει συμφωνηθεί στην ΕΕ. Αφού ελέγχετε ο κωδικός QR, εμφανίζονται μόνο η κατάσταση του πιστοποιητικού, το όνομα και η ημερομηνία γέννησης.
- **Κρυπτογραφική ασφάλεια**: Ο κωδικός QR προστατεύεται με ισχυρή υπογραφή και δεν μπορεί να πλαστογραφηθεί.

6.3.4 Έλεγχος της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.8) παρατηρείται ότι δεν έχει βρεθεί ιχνηλάτης (trackers).

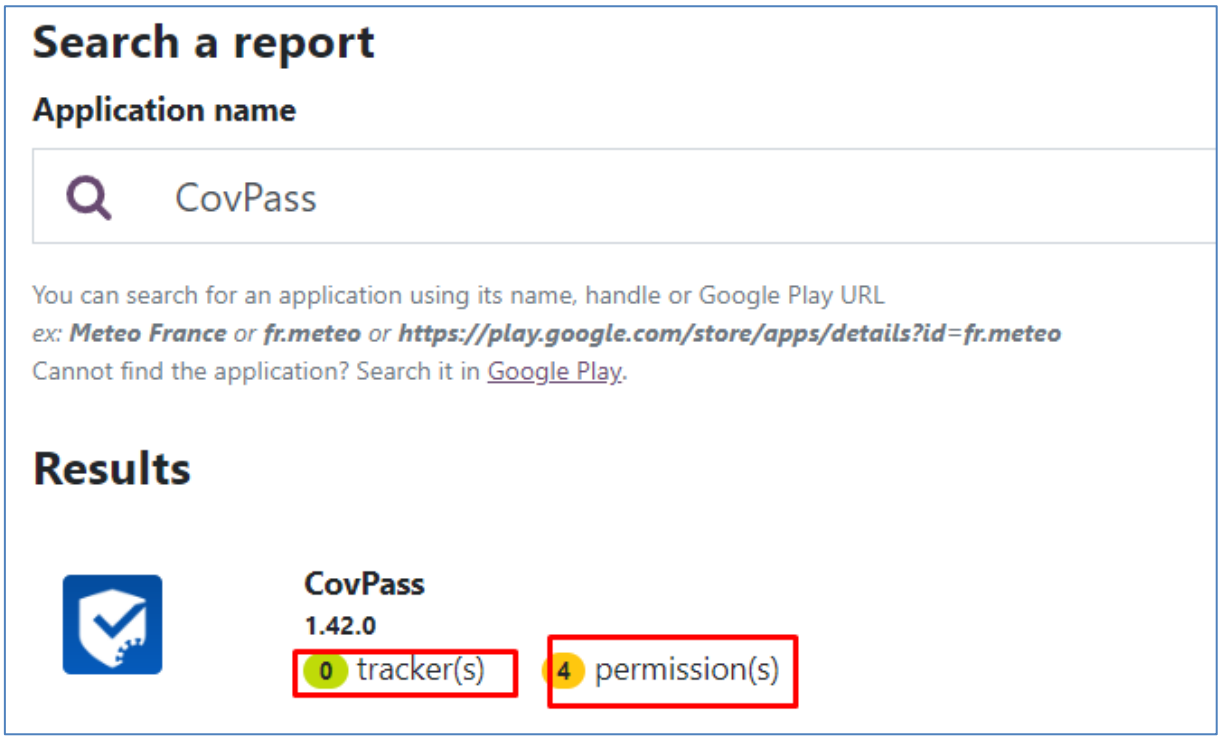
Όσον αφορά τις άδειες / δικαιώματα έχει 4 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Foreground_Service: εκτέλεση υπηρεσίας προσκηνίου
4. Internet: για πλήρη πρόσβαση στο δίκτυο

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovPass, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας.

Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Βέβαια στην ιστοσελίδα: https://wiki.eudcc.gov.cy/en/privacy.php/ όπου καταγράφονται τα privacy policy της εφαρμογής CovPass δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovPass: «*Η εφαρμογή «CovPass» που φιλοξενεί το ψηφιακό πιστοποιητικό Covid, εφεξής «η εφαρμογή» δημιουργήθηκε για την εφαρμογή του Κανονισμού (ΕΕ) 2021/953. Ο παρών κανονισμός προβλέπει την αμοιβαία αναγνώριση των πιστοποιητικών που εκδίδονται από τα κράτη μέλη της ΕΕ στους πολίτες για τη διευκόλυνση της ελεύθερης κυκλοφορίας τους μεταξύ κρατών μελών. Τα προσωπικά σας δεδομένα που καταχωρούνται σε αυτό θα υποβάλλονται σε επεξεργασία σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, εφεξής «GDPR» και της Προστασίας Φυσικών Προσώπων σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και την Ελεύθερη Διακίνηση Τέτοιου Δεδομένων Νόμου του 2018, Ν.125(Ι)/2018, εφεξής «η Εθνική Νομοθεσία», αμφότερα αποτελούν «το νομοθετικό πλαίσιο για την προστασία ή τα προσωπικά δεδομένα»*)» (CovPass / privacy policy, 2021)



Εικόνα 6.8: Έλεγχος της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy.

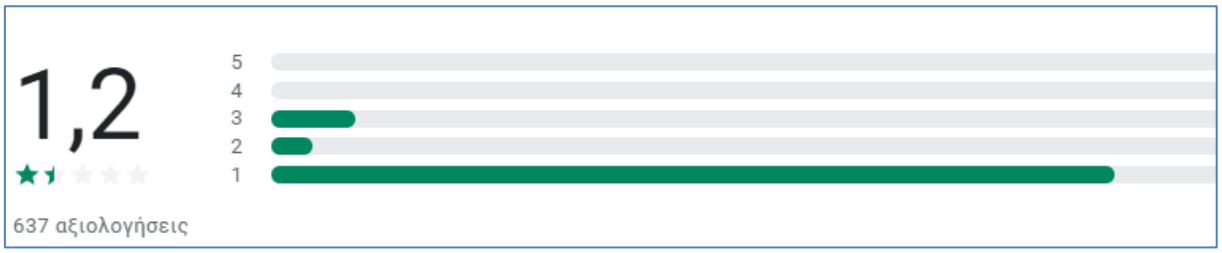
6.4 CovScan Cyprus

Η επίσημη αίτηση της Κυπριακής Κυβέρνησης για την επαλήθευση της εγκυρότητας ενός Digital ψηφιακού Πιστοποιητικού COVID της ΕΕ (EUDCC) για οικιακή χρήση αποτελεί η εφαρμογή CovScan Cyprus (CovScan Cyprus, 2021).

Εικόνα 6.9: Όνομα και λογότυπο της εφαρμογής CovScan Cyprus.

6.4.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovScan Cyprus από τους 637 περίπου αξιολογητές / χρήστες της, στην ιστοσελίδα Google Play είναι 1,2/5 (εικόνα 6.10) (CovPass, 2021).



Εικόνα 6.10: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovScan Cyprus,
από τους 637 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.4.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια του εκάστοτε χρήστη της εφαρμογής CovScan ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (CovScan Cyprus, 2021).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.4.3 Έλεγχος της εφαρμογή CovScan Cyprus με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή CovScan με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.11) παρατηρείται ότι έχουν βρεθεί 2 ιχνηλάτες (trackers):

α) Microsoft Visual Studio App Center Analytics[13]: Συλλέγει αναλυτικά στοιχεία σε πραγματικό χρόνο που τονίζουν τη συμπεριφορά των χρηστών. Παρέχει επίσης ειδοποιήσεις push σε κινητές συσκευές.

β) Microsoft Visual Studio App Center Crashes (crash reporting/ αναφορά σύγκρουσης)[14]: Δημιουργεί αυτόματα ένα αρχείο καταγραφής σφαλμάτων κάθε

[13] Κανόνες ανίχνευσης:

- Κανόνας ανίχνευσης κώδικα: com.microsoft.appcenter.analytics | com.microsoft.azure.mobile.analytics
- Κανόνας ανίχνευσης δικτύου: NC

[14] Κανόνες ανίχνευσης

φορά που η εφαρμογή σας διακόπτεται. Το αρχείο καταγραφής γράφεται πρώτα στο χώρο αποθήκευσης της συσκευής και όταν ο χρήστης ξεκινήσει ξανά την εφαρμογή, το αρχείο καταγραφής σφαλμάτων θα σταλεί στο App Center.

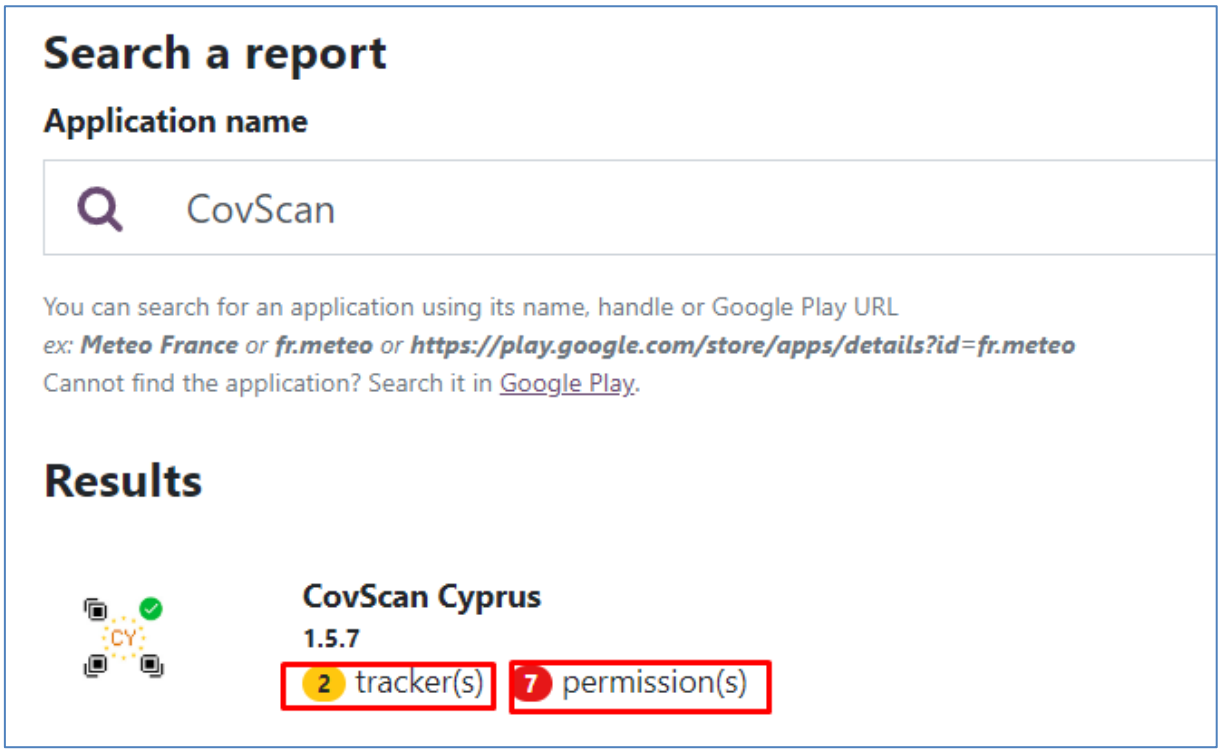
Όσον αφορά τις άδειες / δικαιώματα έχει 7 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Foreground_Service: εκτέλεση υπηρεσίας προσκηνίου
4. Internet: για πλήρη πρόσβαση στο δίκτυο
5. Receive Boot Completed: λειτουργία κατά την εκκίνηση
6. Reorder Tasks: αναδιάταξη εφαρμογών που εκτελούνται
7. Wake Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε αδράνεια / αναστολή

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovScan, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Βέβαια στην ιστοσελίδα: https://wiki.eudcc.gov.cy/en/privacy.php/ όπου καταγράφονται τα privacy policy της εφαρμογής CovScan δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovPass: «*Η εφαρμογή «CovScan» έχει σχεδιαστεί για την εκτέλεση της επαλήθευσης/ελέγχου της γνησιότητας, εγκυρότητας και ακεραιότητας των ψηφιακών πιστοποιητικών Covid-19, εφεξής «η εφαρμογή», η οποία βασίζεται στο πλαίσιο της εφαρμογής του Κανονισμού. ΕΕ) 2021/953 και των Λοιμωδών Νοσημάτων (Καθορισμός Μέτρων για την Πρόληψη της Εξάπλωσης του Κορωνοϊού COVID-19 Διάταγμα του 2021) Διατάγματα, που εκδόθηκαν από τον Υπουργό Υγείας της Κυπριακής Δημοκρατίας*» (CovPass / privacy policy, 2021).

- Κανόνας ανίχνευσης κώδικα: com.microsoft.appcenter.crashes
- Κανόνας ανίχνευσης δικτύου: NC



Εικόνα 6.11: Έλεγχος της εφαρμογή CovScan με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/CovScan Cyprus, 2023)*.

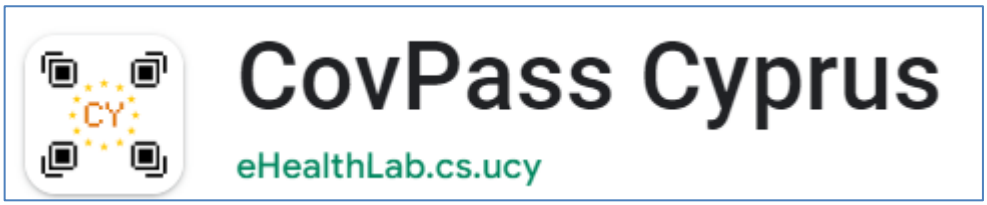
6.5 CovPass Cyprus

Η CovPass Cyprus αποτελεί την επίσημη εφαρμογή ηλεκτρονικού πορτοφολιού της Κυπριακής Κυβέρνησης όπου οι χρήστες μπορούν να σαρώσουν, να αποθηκεύσουν και να έχουν πρόσβαση στο Digital ψηφιακό πιστοποιητικό COVID της ΕΕ (EUDCC).

Ισχύει μόνο για χρήστες των οποίων το EUDCC εκδόθηκε στην Κύπρο και περιέχει κωδικό TAN (transaction authentication number)[15] (CovPass Cyprus, 2021).

[15] Ένας αριθμός ελέγχου ταυτότητας συναλλαγής (transaction authentication number / TAN) χρησιμοποιείται από ορισμένες διαδικτυακές τραπεζικές υπηρεσίες ως μια μορφή κωδικών πρόσβασης μίας χρήσης (one-time passwords / OTP) για την εξουσιοδότηση οικονομικών συναλλαγών. Ο TAN είναι ένα δεύτερο επίπεδο ασφάλειας πάνω και πέρα από τον παραδοσιακό έλεγχο ταυτότητας με έναν κωδικό πρόσβασης.

Οι TAN παρέχουν πρόσθετη ασφάλεια επειδή λειτουργούν ως μια μορφή ελέγχου ταυτότητας δύο παραγόντων (two-factor authentication / 2FA). Εάν το φυσικό έγγραφο ή το διακριτικό που περιέχει τα TAN κλαπεί, θα είναι άχρηστο χωρίς τον κωδικό πρόσβασης. Αντίθετα, εάν ληφθούν τα δεδομένα σύνδεσης, καμία συναλλαγή δεν μπορεί να πραγματοποιηθεί χωρίς έγκυρο TAN.



Εικόνα 6.12: Όνομα και λογότυπο της εφαρμογής CovPass Cyprus.

6.5.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass Cyprus από τους 1120 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,4/4 (εικόνα 6.13) (CovPass Cyprus, 2021).

Εικόνα 6.13: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass Cyprus, από τους 1120 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.5.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια του εκάστοτε χρήστη της εφαρμογή CovPass ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (CovPass Cyprus, 2021).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.5.3 Έλεγχος της εφαρμογή CovPass Cyprus με το διαδικτυακό εργαλείο Exodus Privacy

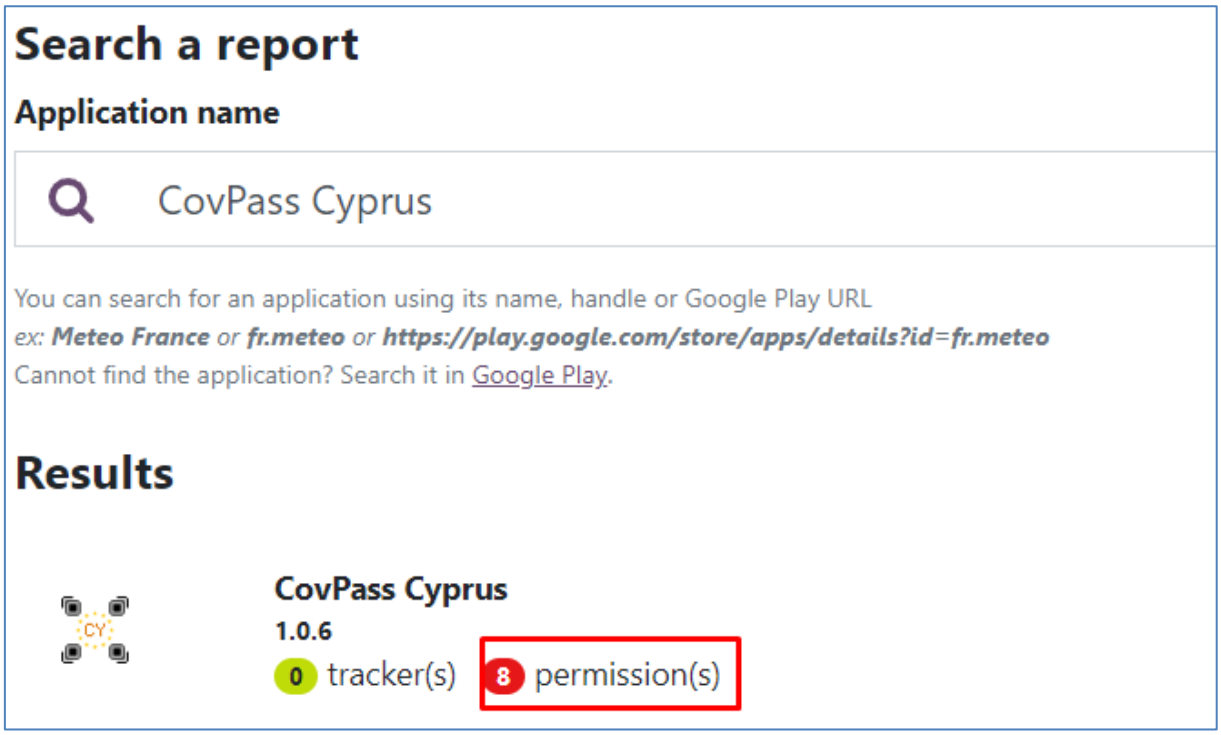
Κατά τον έλεγχο της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.14) παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers).

Όσον αφορά τις άδειες / δικαιώματα έχει 8 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Foreground_Service: εκτέλεση υπηρεσίας προσκηνίου
4. Internet: για πλήρη πρόσβαση στο δίκτυο
5. Receive Boot Completed: λειτουργία κατά την εκκίνηση
6. Use_Biometric: χρησιμοποιεί βιομετρικό υλικό
7. Use_Fingerprint: χρησιμοποιεί δακτυλικά αποτυπώματα
8. Wake Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε αδράνεια / αναστολή

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovPass, το δικαίωμα «Camera» , το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Αναμφίβολα στην ιστοσελίδα: https://wiki.eudcc.gov.cy/en/privacy.php/ όπου καταγράφονται τα privacy policy της εφαρμογής CovPass δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovPass: «*Η εφαρμογή «CovPass» που φιλοξενεί το ψηφιακό πιστοποιητικό Covid, εφεξής «η εφαρμογή» δημιουργήθηκε για την εφαρμογή του Κανονισμού (ΕΕ) 2021/953. Ο παρών κανονισμός προβλέπει την αμοιβαία αναγνώριση των πιστοποιητικών που εκδίδονται από τα κράτη μέλη της ΕΕ στους πολίτες για τη διευκόλυνση της ελεύθερης κυκλοφορίας τους μεταξύ κρατών μελών. Τα προσωπικά σας δεδομένα που καταχωρούνται σε αυτό θα υποβάλλονται σε επεξεργασία σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, εφεξής «GDPR» και της Προστασίας Φυσικών Προσώπων σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και την Ελεύθερη Διακίνηση Τέτοιου Δεδομένων Νόμου του 2018, Ν.125(Ι)/2018, εφεξής «η Εθνική Νομοθεσία», αμφότερα αποτελούν «το νομοθετικό πλαίσιο για την προστασία ή τα προσωπικά δεδομένα»*)» (CovPass / privacy policy, 2021).



Εικόνα 6.14: Έλεγχος της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/CovScan Cyprus, 2023)*.

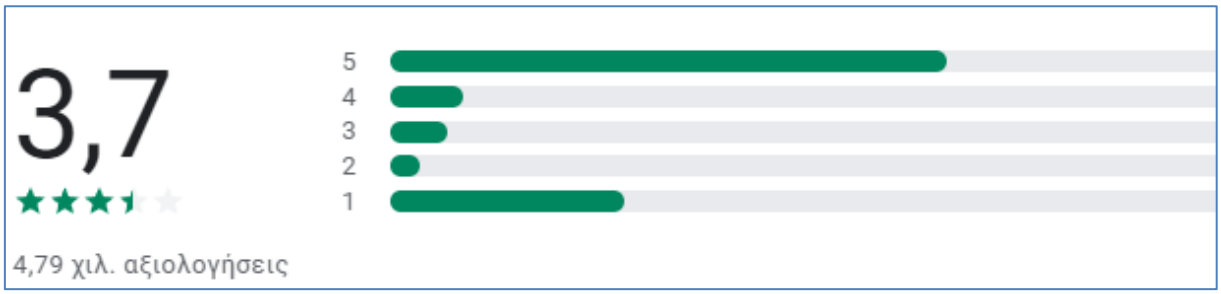
6.6 Covid Free GR

Η εφαρμογή Covid Free GR αποτελεί την επίσημη ελληνική εφαρμογή για την επιβεβαίωση ευρωπαϊκών ψηφιακών πιστοποιητικών COVID και είναι διαθέσιμη μέσω του επίσημου λογαριασμού της Ελληνικής Δημοκρατίας (Covid Free GR Wallet/Hellenic Republic, 2021).

Εικόνα 6.15: Όνομα και λογότυπο της εφαρμογής Covid Free GR.

6.6.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Covid Free GR από τους 4790 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 3,7/5 (εικόνα 6.16) (Covid Free GR Wallet/Hellenic Republic, 2021).



Εικόνα 6.16: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Covid Free GR,

από τους 4790 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.6.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια του εκάστοτε χρήστη της εφαρμογή Covid Free GR ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (Covid Free GR Wallet/Hellenic Republic, 2021).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.6.3 Έλεγχος της εφαρμογή Covid Free GR με το διαδικτυακό εργαλείο Exodus Privacy

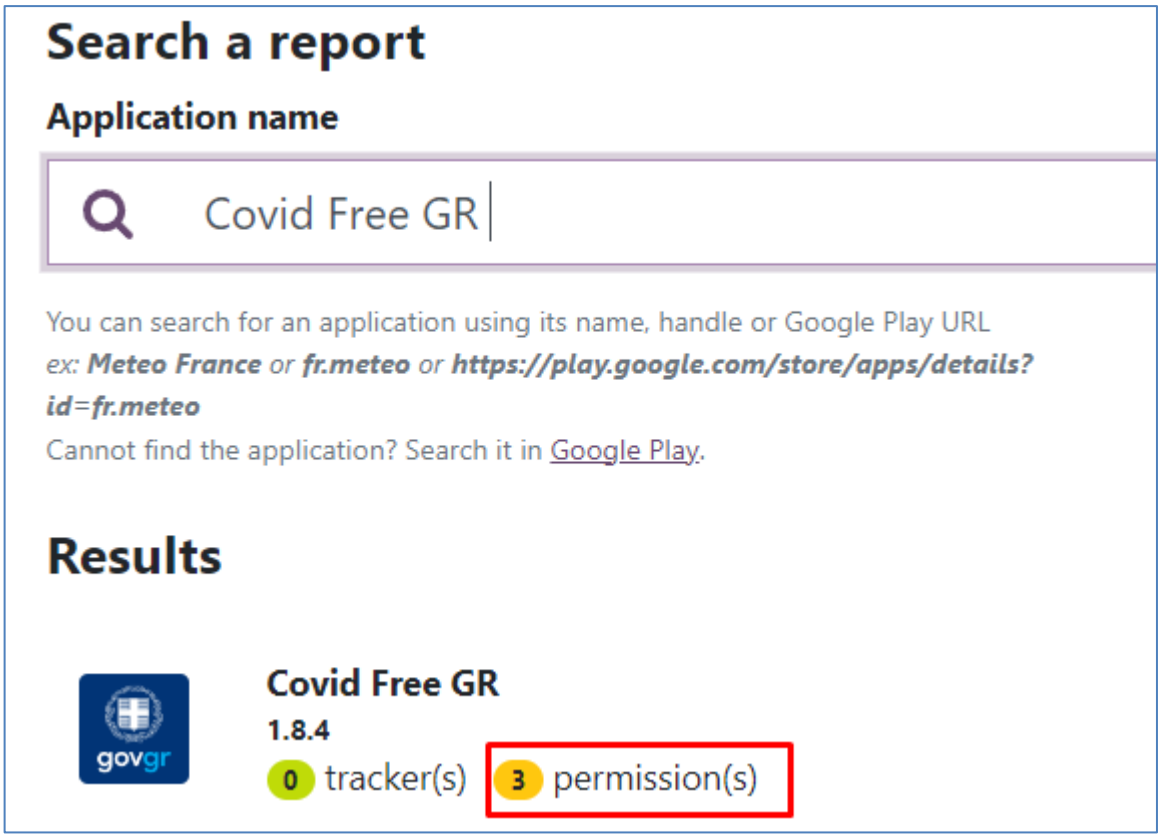
Κατά τον έλεγχο της εφαρμογή Covid Free GR με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.17) παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers).

Όσον αφορά τις άδειες / δικαιώματα έχει 3 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Camera: για φωτογραφίες και βίντεο
3. Internet: για πλήρη πρόσβαση στο δίκτυο

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Covid Free GR, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει» τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Αναμφίβολα στην ιστοσελίδα: https://covidfree.gov.gr/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής Covid Free GR δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Ομόγνωμα με το τμήμα privacy policy της εφαρμογής Covid Free GR: «*Η Ανεξάρτητη Αρχή με την επωνυμία «ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ» (ΕΑΔ) υπό την ιδιότητά της ως Υπεύθυνης Επεξεργασίας των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας κατά τη λειτουργία της ειδικής ηλεκτρονικής εφαρμογής για τον έλεγχο της εγκυρότητας, της γνησιότητας και της ακεραιότητας του Ψηφιακού Πιστοποιητικού COVID -19 της Ε.Ε. (EU Digital COVID Certificate - EUDCC) και της βεβαίωσης εμβολιασμού της παρ. 5 του άρθρου 55 του ν. 4764/2020 (Α' 256) ή ισοδύναμου πιστοποιητικού ή βεβαίωσης, που φέρει το φυσικό πρόσωπο - κάτοχος, διά της σάρωσης του σχετικού κωδικού QR, με τη χρήση της ειδικής ηλεκτρονικής εφαρμογής CovidFreeGr, εγγυάται τον σεβασμό της ιδιωτικότητας των φυσικών προσώπων καθώς και την προστασία των προσωπικών τους δεδομένων*» (Covid Free GR /privacy policy, 2021).



Εικόνα 6.17: Έλεγχος της εφαρμογή Covid Free GR με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/Covid Free GR, 2023)*

6.7 MyHealth

Η εφαρμογή MyHealth αποτελεί τον ηλεκτρονικό Ιατρικό Φάκελο Ασθενούς στην Ελλάδα.

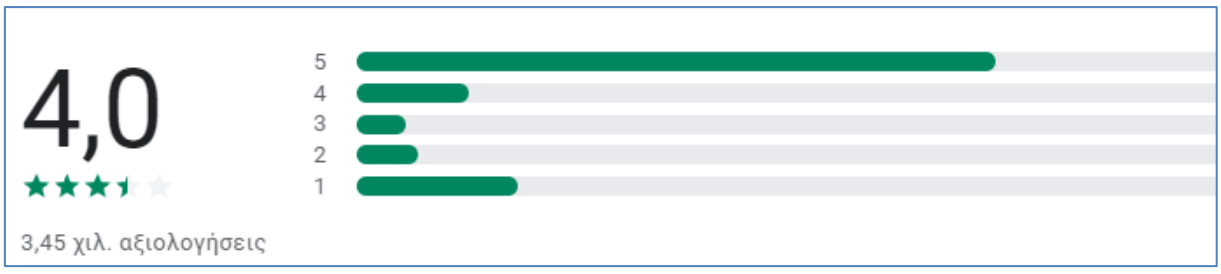
Εικόνα 6.18: Όνομα και λογότυπο της εφαρμογή MyHealth.

Η εφαρμογή MyHealth δίνει την δυνατότητα στους χρήστες να:

- εκδώσουν αποτελέσματα ιατρικών εξετάσεων και βεβαιώσεων νοσηλείας ή της επίσκεψης αλλά και βεβαιώσεις εργαστηριακών εξετάσεων από δημόσιες και ιδιωτικές μέσω του gov.gr.
- διαχειριστούν μαζεμένες τις πληροφορίες που αφορούν τις συνταγές και τα παραπεμπτικά τους
- έχουν άμεση και εύκολη πρόσβαση στο ιστορικό της άυλης συνταγογράφησης και να λαμβάνουν ειδοποιήσεις μέσω Push Notifications για τις νέες συνταγές και παραπεμπτικά εξετάσεων

6.7.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή MyHealth από τους 3450 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,0/5 (εικόνα 6.19) (Google Play / MyHealth, 2022).



Εικόνα 6.19: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή MyHealth,

από τους 3450 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.7.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια του εκάστοτε χρήστη στην εφαρμογή MyHealth ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (Google Play / MyHealth, 2022).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.7.3 Έλεγχος της εφαρμογή MyHealth με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή MyHealth με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.20) παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers).

Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 17 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Access_Wifi_State: πλήρη πρόσβαση στο δίκτυο Wi-Fi
3. Foreground_Service: εκτέλεση υπηρεσίας σε πρώτο πλάνο
4. Internet: έχει πλήρη πρόσβαση στο δίκτυο
5. Read_External_Storage: διαβάζει τα περιεχόμενα του κοινόχρηστου αποθηκευτικού χώρου
6. Receive_Boot_Completed: λειτουργία κατά την εκκίνηση
7. Request_Ignore_Battery_Optimizations: ζητά να αγνοήσει ο χρήστης τις βελτιστοποιήσεις μπαταρίας
8. System_Alert_Window: Αυτή η εφαρμογή μπορεί να εμφανίζεται πάνω από άλλες εφαρμογές
9. Use_Biometric: χρησιμοποιεί βιομετρικό υλικό
10. Use_Fingerprint: χρησιμοποιεί υλικό δακτυλικών αποτυπωμάτων
11. Use_Full_Screen_Intent: εμφανίζει ειδοποιήσεις ως δραστηριότητες πλήρους οθόνης σε κλειδωμένη συσκευή
12. Vibrate: ελέγχει την δόνηση

13. Wake_Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε κατάσταση αναστολής
14. Write_External_Storage: τροποποιεί ή διαγράφει τα περιεχόμενα του κοινόχρηστου αποθηκευτικού χώρου
15. Write_Settings: τροποποιεί τις ρυθμίσεις συστήματος
16. Receive: λαμβάνει αυτόματα περιεχόμενο στοιχείων
17. Bind_Get_Install_Referrer_Service: Σύνδεση Λήψη Εγκατάστασης

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύονται 4 επικίνδυνα δικαιώματα (high-risk permissions) της εφαρμογής MyHealth, και αυτά είναι: Read_External_Storage, System_Alert_Window, Write_External_Storage, Write_Settings.

Τα οποία σύμφωνα με την ερευνήτρια: το Read_External_Storage το οποίο διαβάζει τον Εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό υγείας), το Write External Storage με το οποίο η εφαρμογή έχει την δυνατότητα εγγραφής σε εξωτερική αποθηκευτική μονάδα του smartphone (προφανώς πιστοποιητικού υγείας), το Write Settings με το οποίο η εφαρμογή ρυθμίζει εγγραφή του εκάστοτε πιστοποιητικού υγείας στο smartphone και το System Alert Window το οποίο αποτελεί «παράθυρο» ειδοποίησης συστήματος για κάθε μεταβολή της εφαρμογής δεν αποτελούν απειλή σύμφωνα με τις παραπάνω διεργασίες που κατεγράφησαν.

Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Βέβαια στην ιστοσελίδα: https://myhealth.gov.gr/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής MyHealth δεν αναφέρονται τα παραπάνω επικίνδυνα δικαιώματα, με την εξής δήλωση: «*Το Υπουργείο Υγείας υπό την ιδιότητά του ως Υπεύθυνος Επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας κατά τη λειτουργία της ειδικής ηλεκτρονικής εφαρμογής για κινητές συσκευές (mobile application) «myHealth» εγγυάται τον σεβασμό της ιδιωτικότητας των φυσικών προσώπων καθώς και την προστασία των προσωπικών τους δεδομένων*» (mobile application) «myHealth», 2021).

Εικόνα 6.20: Έλεγχος της εφαρμογή MyHealth με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/MyHealth, 2023)*.

6.8 COVID Alert NJ

Η εφαρμογή COVID Alert NJ διατίθεται από το Υπουργείο Υγείας του Νιου Τζέρσεϋ (Department of Health / DOH) των ΗΠΑ για να συμπληρώσει την ολοκληρωμένη προσπάθεια ανίχνευσης επαφών COVID-19 του Νιου Τζέρσεϋ.

Εικόνα 6.21: Όνομα και λογότυπο της εφαρμογής COVID Alert NJ.

Η COVID Alert NJ είναι μια δωρεάν και ασφαλής εφαρμογή για κινητά τηλέφωνα που επιτρέπει στους κατοίκους της πολιτείας των ΗΠΑ Νιου Τζέρσεϋ (COVID Alert NJ, 2020):

1. Να λαμβάνουν ειδοποίηση εάν ήταν σε στενή επαφή με άλλο χρήστη της εφαρμογής που έχει δείξει θετικό για το COVID-19 - ακόμη και αν αυτό το άτομο είναι ξένος.

2. Να παρακολουθούν τα συμπτώματά τους και να λαμβάνουν συμβουλές για το τι πρέπει να κάνουν για να προστατεύσουν τον εαυτό τους και τους άλλους.

3. Να μπορούν να προειδοποιούν ανώνυμα άλλους χρήστες εφαρμογών με τους οποίους ήρθαν σε στενή επαφή, εάν έδειξαν θετικό για το COVID-19 - ειδικά άτομα με τα οποία δεν γνωρίζουν ή θυμούνται να βρίσκονται σε στενή επαφή (π.χ. κατά τη διάρκεια της διαδρομής με λεωφορείο / τρένο, σε δημόσιους χώρους).

4. Για την παρακολούθηση των τελευταίων πληροφοριών και στατιστικών που σχετίζονται με την πανδημία COVID-19.

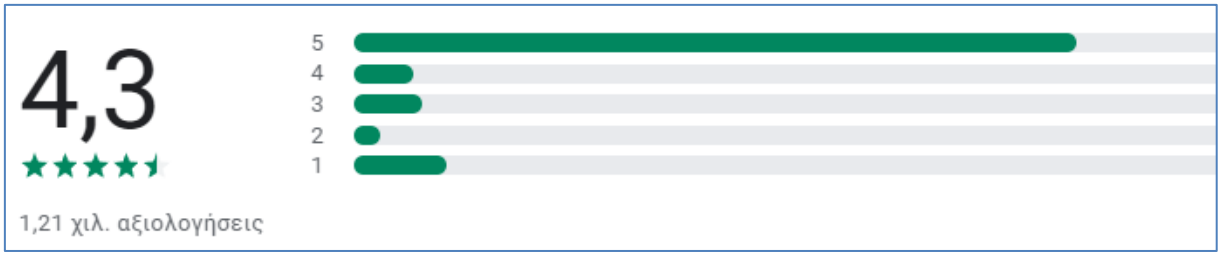
5. Για να επικοινωνήσουν με εκπροσώπους της δημόσιας υγείας του NJ και να συνδεθούν με υπηρεσίες υποστήριξης

Για να λειτουργήσουν όλα αυτά, το μόνο που πρέπει να κάνει ο εκάστοτε χρήστης είναι να πιέσετε το «Allow» COVID-19 Exposure Notification Services (ENS) στο τηλέφωνό του μέσα στην εφαρμογή του.

Μπορεί επίσης να επιλέξει «Να επιτρέπεται» στο τηλέφωνό του για να ενεργοποιήσει τις υπηρεσίες ειδοποίησης έκθεσης COVID-19 (ENS) και επίσης να «επιτρέψει» στο τηλέφωνό του να εμφανίζει ειδοποιήσεις, ώστε να λαμβάνει επίσης μια ειδοποίηση ότι έχει εκτεθεί σε κάποιον που έχει δηλωθεί θετικός στον COVID-19. Μπορεί επίσης να απενεργοποιήσει αυτήν τη λειτουργία, ανά πάσα στιγμή, στη σελίδα Ρυθμίσεις της εφαρμογής.

6.8.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή COVID Alert NJ από τους 8980 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,3/5 (εικόνα 6.22) (COVID Alert NJ, 2020).



Εικόνα 6.22: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή COVID Alert NJ,

από τους 1210 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.8.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Είναι σημαντικό να σημειωθεί ότι η εφαρμογή COVID Alert NJ δεν αποκαλύπτει ποτέ την ταυτότητα οποιουδήποτε ατόμου που χρησιμοποιεί την εφαρμογή σε άλλους χρήστες

της εφαρμογής και ποτέ δεν αποκαλύπτει ποιος έχει διαγνωστεί ως θετικός για το COVID-19 (COVID Alert NJ, 2020).

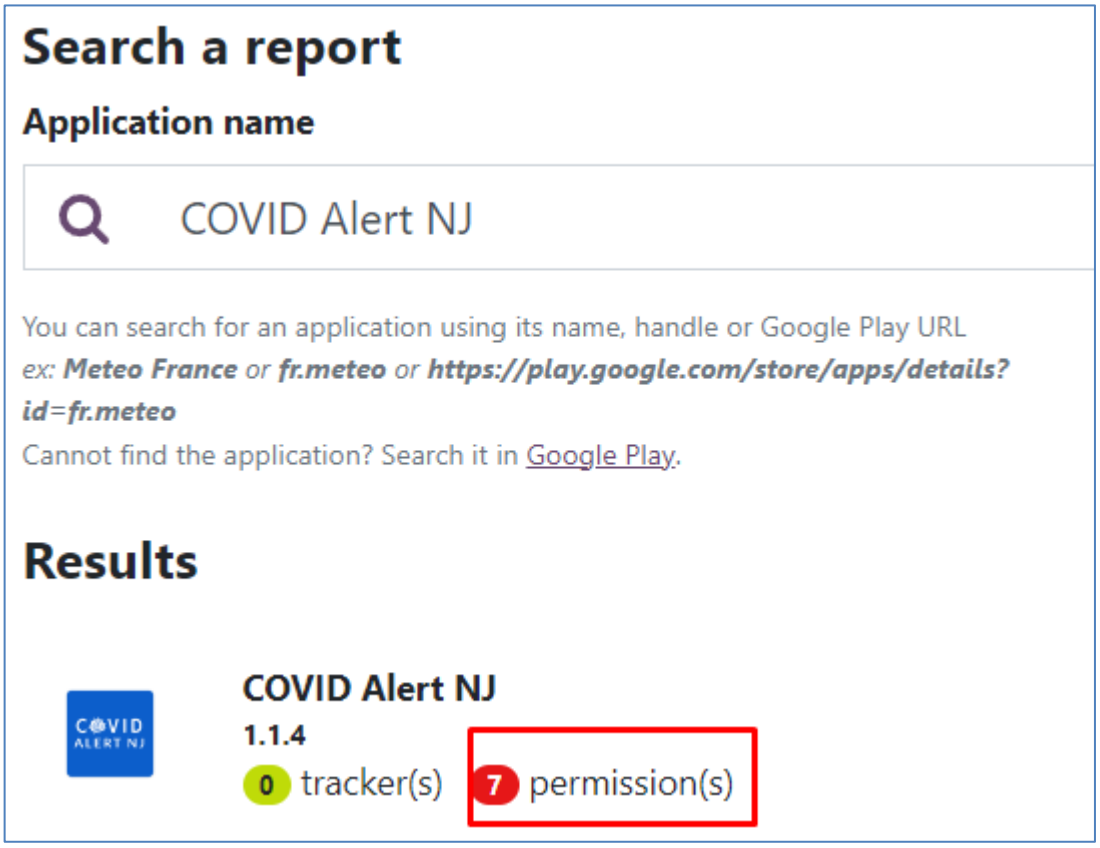
6.8.3 Έλεγχος της εφαρμογή COVID Alert NJ με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή COVID Alert NJ με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.23) παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers).

Όσον αφορά τις άδειες / δικαιώματα έχει 7 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Access_Wifi_State: προβολή συνδέσεων Wi-Fi
3. Bluetooth: σύζευξη με συσκευές Bluetooth
4. Foreground_Service: εκτέλεση υπηρεσίας πρώτου πλάνου
5. Internet: έχει πλήρη πρόσβαση στο δίκτυο
6. Receive_Boot_Completed: λειτουργεί κατά την εκκίνηση
7. Vibrate: έλεγχος των κραδασμών / δόνησης

Σύμφωνα με τα επίπεδα προστασίας της Google δεν υποδεικνύεται κανένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή COVID Alert NJ.



Εικόνα 6.23: Έλεγχος της εφαρμογή COVID Alert NJ με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/COVID Alert NJ, 2023)*.

6.9 WHO Info

Με την εφαρμογή WHO Info/World Health Organization, η οποία αποτελεί την επίσημη εφαρμογή πληροφοριών του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ - WHO / World Health Organization), ο εκάστοτε χρήστης έχει τις τελευταίες πληροφορίες για την υγεία στο τηλέφωνό του. Αυτή η εφαρμογή εμφανίζει τις τελευταίες ειδήσεις, εκδηλώσεις, δυνατότητες και σημαντικές ενημερώσεις σχετικά με τα κρούσματα της εκάστοτε πανδημίας, όπως του COVID.

Εικόνα 6.24: Όνομα και λογότυπο της εφαρμογής WHO Info/World Health Organization.

Ο ΠΟΥ εργάζεται παγκοσμίως για να προάγει την υγεία, να διατηρεί τον κόσμο ασφαλή και να εξυπηρετεί τους ευάλωτους ανθρώπους.

Στόχος του είναι να διασφαλίσει ότι ένα δισεκατομμύριο περισσότεροι άνθρωποι θα έχουν καθολική κάλυψη υγείας, θα προστατεύουν ένα δισεκατομμύριο περισσότερους ανθρώπους από καταστάσεις έκτακτης ανάγκης στην υγεία και θα παρέχουν σε άλλα δισεκατομμύρια άτομα καλύτερη υγεία και ευεξία (WHO Info, 2020).

6.9.1 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια της εφαρμογής WHO Info/World Health Organization του εκάστοτε χρήστη ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (WHO Info, 2020).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.9.2 Έλεγχος της εφαρμογή WHO Info με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή WHO Info με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.25) παρατηρείται ότι έχει βρεθεί 1 ιχνηλάτης (trackers), ο Google Firebase Analytics: Το Firebase προσφέρει λειτουργίες όπως αναλυτικά (στατιστικά) στοιχεία, βάσεις δεδομένων, ανταλλαγή μηνυμάτων και αναφορές σφαλμάτων[16].

Ασφαλώς στην ιστοσελίδα: https://www.who.int/about/policies/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής WHO Info δεν αναφέρονται ο παραπάνω επικίνδυνος ιχνηλάτης. Σύμφωνα με το τμήμα privacy policy της εφαρμογής WHO Info: «*Οι πληροφορίες που συλλέγονται κατά τη γενική περιήγηση στον τομέα "who.int" χρησιμοποιούνται για την ανάλυση των τάσεων και της χρήσης του ιστότοπου του ΠΟΥ και για τη βελτίωση της χρησιμότητας του ιστότοπου. Δεν συνδέεται με καμία προσωπική πληροφορία …. Δεν πουλάμε ούτε κοινοποιούμε οποιεσδήποτε προσωπικές πληροφορίες που παρέχονται εθελοντικά στον ιστότοπο του ΠΟΥ σε κανένα τρίτο μέρος*» (Privacy policy / WHO Info, 2021).

Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 9 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Access_Wifi_State: πλήρη πρόσβαση στο δίκτυο Wi-Fi
3. Read_Calendar: διαβάζει συμβάντα και λεπτομέρειες ημερολογίου
4. Read_External_Storage: διαβάζει τα περιεχόμενα του κοινόχρηστου αποθηκευτικού χώρου
5. Wake_Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε αναστολή λειτουργίας
6. Write_Calendar: προσθέτει ή τροποποιεί συμβάντα ημερολογίου και στέλνει email στους επισκέπτες χωρίς να το γνωρίζουν οι κάτοχοι
7. Write_External_Storage: τροποποιεί ή διαγράφει τα περιεχόμενα του κοινόχρηστου αποθηκευτικού χώρου
8. Receive: λαμβάνουν αυτόματα περιεχόμενο στοιχείων
9. Bind_Get_Install_Referrer_Service: Σύνδεση Λήψη Εγκατάστασης

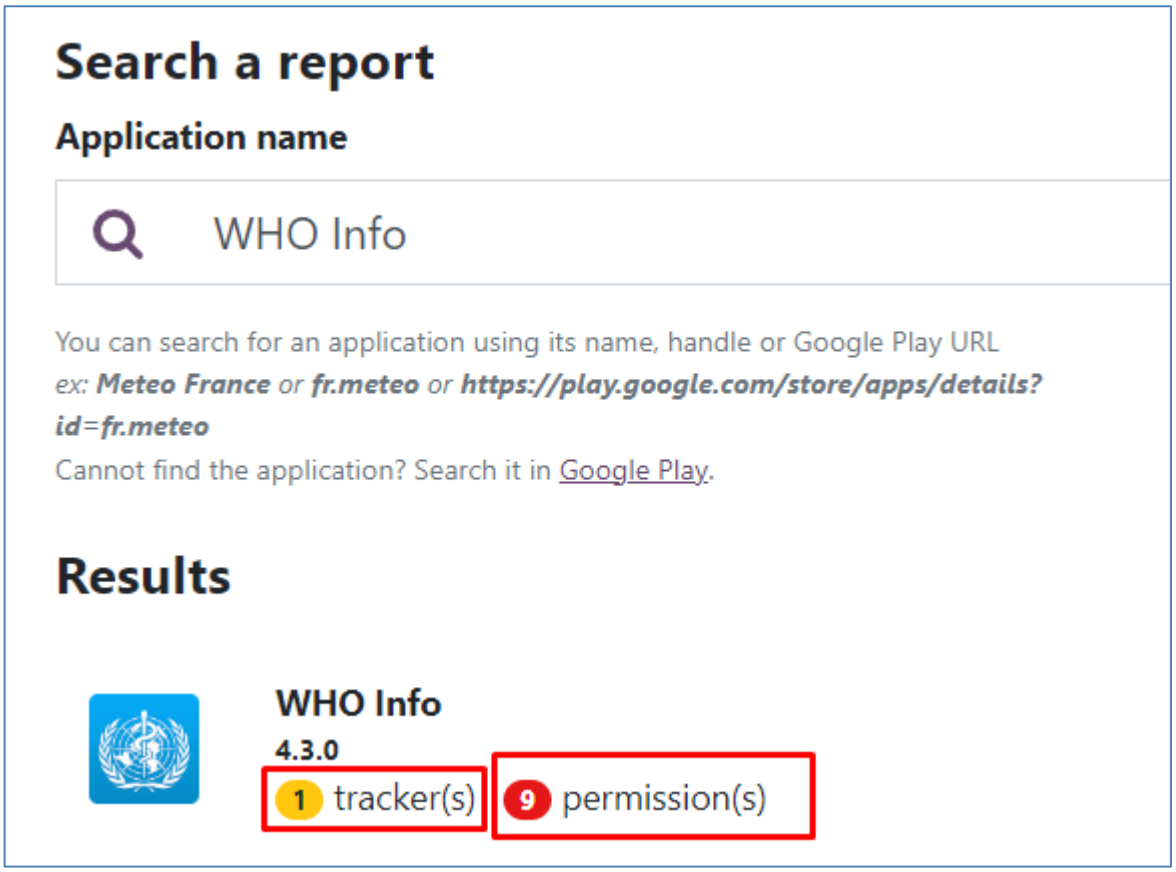
Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύονται 4 επικίνδυνα δικαιώματα (high-risk permissions) της εφαρμογή WHO Info, όπως τα: Read_Calendar,

[16] Κανόνες ανίχνευσης:

- Κανόνας ανίχνευσης κώδικα: com.google.firebase.analytics. | com.google.android.gms.measurement. | com.google.firebase.firebase_analytics
- Κανόνας ανίχνευσης δικτύου: firebase\.com

Read_External_Storage, Write_Calendar, Write_External_Storage, τα οποία σύμφωνα με την ερευνήτρια δεν αποτελούν απειλή διότι είναι απόλυτα αναμενόμενα αφού με το δικαίωμα Read Calendar η εφαρμογή διαβάζει την χρονική διάρκεια των πιστοποιητικών υγείας και ενημερώνεται για την λήξη αυτών, με το δικαίωμα Read External Storage η εφαρμογή διαβάζει τον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό υγείας), με το δικαίωμα Write Calendar η εφαρμογή γράφει την χρονική διάρκεια των πιστοποιητικών υγείας και ενημερώνεται για την λήξη αυτών, τέλος με το δικαίωμα Write External Storage γράφει στον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς πιστοποιητικό υγείας). Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Από το τμήμα privacy policy της εφαρμογής WHO Info δεν προκύπτει αναγκαιότητα των επικίνδυνων δικαιωμάτων (high-risk permissions) σύμφωνα με τα επίπεδα προστασίας της Google. Δηλαδή στην ιστοσελίδα: https://www.who.int/about/policies/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής WHO Info, εκτός των άλλων αναφέρονται: «*Οποιεσδήποτε πληροφορίες παρέχονται στον ΠΟΥ από χρήστες του ιστότοπου του ΠΟΥ τηρούνται με τη μέγιστη προσοχή και ασφάλεια και δεν θα χρησιμοποιηθούν με τρόπους διαφορετικούς από εκείνους που ορίζονται στην παρούσα πολιτική απορρήτου ή σε πολιτικές ειδικές για τον ιστότοπο ή με τρόπους που έχετε ρητά συναινέσει. Ο ΠΟΥ χρησιμοποιεί μια σειρά τεχνολογιών και μέτρων ασφαλείας για την προστασία των πληροφοριών που διατηρούνται στα συστήματά μας από απώλεια, κακή χρήση, μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη, τροποποίηση ή καταστροφή*» (Privacy policy / WHO Info, 2021).



Εικόνα 6.25: Έλεγχος της εφαρμογή WHO Info με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/WHO Info, 2023)*.

6.10 OpenWHO

Η εφαρμογή OpenWHO: Knowledge for Health είναι η πλατφόρμα διαδραστικής μεταφοράς γνώσης της Παγκόσμιας Οργάνωσης Υγείας (WHO) που προσφέρει online μαθήματα για τη βελτίωση της ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης για την υγεία. Το OpenWHO επιτρέπει στον Οργανισμό και στους βασικούς συνεργάτες του να μεταφέρουν τη γνώση διάσωσης σε μεγάλους αριθμούς ανταποκριτών στην πρώτη γραμμή (OpenWHO: Knowledge for Health, 2022).

Εικόνα 6.26: Όνομα και λογότυπο της εφαρμογής OpenWHO: Knowledge for Health.

Με την OpenWHO, ο εκάστοτε χρήστης έχει την ευελιξία να μάθει όσο το δυνατόν καλύτερα ιατρικές πράξεις, παρακολουθώντας σύντομες διαλέξεις βίντεο. Το φόρουμ μαθήματος και ο χώρος συνεργασίας επιτρέπουν στον χρήστη να έρθει σε επαφή με άλλους συμμετέχοντες και εμπειρογνώμονες σε όλο τον κόσμο.

Η εφαρμογή OpenWHO είναι σχεδιασμένη πρωτίστως για τους εργαζόμενους στον τομέα της υγειονομικής περίθαλψης, τους πρώτους ανταποκριτές και τους υπεύθυνους λήψης αποφάσεων, επιπλέον η εφαρμογή αποτελεί επίσης πηγή πληροφόρησης για όσους έχουν πληγεί από εστίες νοσημάτων και καταστάσεις έκτακτης ανάγκης για την υγεία ή για άτομα με γενικό συμφέρον στην εργασία της ΠΟΥ σε περιπτώσεις έκτακτης ανάγκης για την υγεία.

Διαθέτει 6 κανάλια[17] (OpenWHO: Knowledge for Health, 2022):

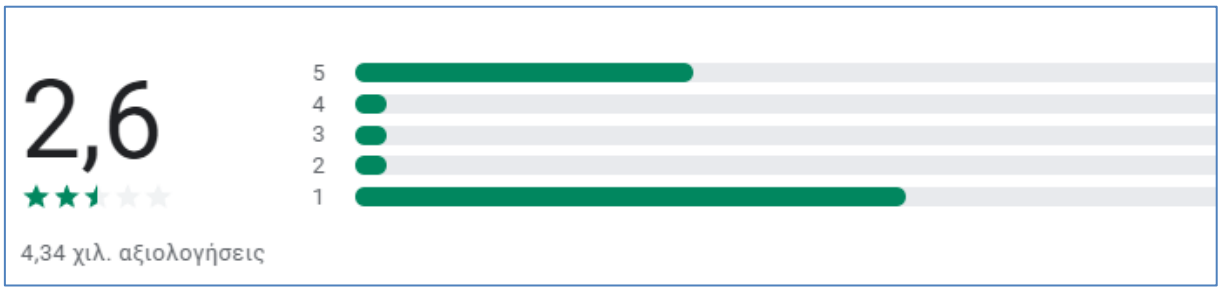
1. Το κανάλι Outbreak απευθύνεται στη διαχείριση των μολυσματικών ασθενειών και παρέχει πληροφορίες ζωτικής σημασίας για την επιστήμη.
2. Το κανάλι Ready / Έτοιμο, για άμεση απόκριση, βοηθάει την προετοιμασία του προσωπικού που εκπαιδεύεται για να εργαστεί σε κρούσματα ασθενειών και καταστάσεις έκτακτης ανάγκης για την υγεία.
3. Το κανάλι Download / Λήψη, κοινωνικού περιεχομένου επικεντρώνεται στις παρεμβάσεις με βάση την κοινωνική επιστήμη και βοηθά στην επικοινωνία με τις επηρεαζόμενες κοινότητες.
4. Το κανάλι Preparation / Προετοιμασία, για πανδημίες συγκεντρώνει μαθήματα σχετικά με διάφορες πτυχές της ετοιμότητας, συμπεριλαμβανομένης της επιτήρησης, των μέτρων δημόσιας υγείας και της επικοινωνίας σχετικά με τον κίνδυνο κατά τη διάρκεια μιας πανδημίας.
5. Το κανάλι COVID-19, το οποίο παρέχει εκπαιδευτικούς πόρους σε 6 επίσημες γλώσσες (αραβικά, κινέζικα, αγγλικά, γαλλικά, ρωσικά και ισπανικά) για τους επαγγελματίες υγείας, τους υπεύθυνους λήψης αποφάσεων και το κοινό για την εκδήλωση της νόσου του κορωναϊού (COVID-19).

[17] Τα μαθήματα OpenWHO είναι διαθέσιμα σε πολλές γλώσσες, συμπεριλαμβανομένων των 6 επίσημων γλωσσών της ΠΟΥ.

6. Το κανάλι COVID-19 των εθνικών γλωσσών παρέχει τους ίδιους μαθησιακούς πόρους με το κανάλι COVID-19, αλλά σε εθνικές γλώσσες, όπως η ινδονησιακή, η ιαπωνική και η πορτογαλική.

6.10.1 Βαθμολογίες και αξιολογήσεις της ιστοσελίδας Google Play

Οι βαθμολογίες και αξιολογήσεις της εφαρμογή OpenWHO από τους 4340 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,6/5 (εικόνα 6.27) (OpenWHO: Knowledge for Health, 2022).



Εικόνα 6.27: Οι βαθμολογίες και αξιολογήσεις της εφαρμογή OpenWHO,

από τους 4340 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play.

6.10.2 Ασφάλεια δεδομένων της ιστοσελίδας Google Play

Η ασφάλεια του εκάστοτε χρήστη στην εφαρμογή OpenWHO ξεκινά από την κατανόηση του τρόπου με τον οποίο οι προγραμματιστές συλλέγουν και κοινοποιούν τα δεδομένα του. Οι πρακτικές απορρήτου και ασφάλειας δεδομένων μπορεί να διαφέρουν ανάλογα με τη χρήση, την περιοχή και την ηλικία του. Αυτές οι πληροφορίες παρέχονται από τον προγραμματιστή και ενδέχεται να ενημερωθούν με την πάροδο του χρόνου (OpenWHO: Knowledge for Health, 2022).

- Δεν κοινοποιούνται δεδομένα σε τρίτα μέρη
- Δεν συλλέγονται δεδομένα

6.10.3 Έλεγχος της εφαρμογή OpenWHO με το διαδικτυακό εργαλείο Exodus Privacy

Κατά τον έλεγχο της εφαρμογή OpenWHO με το διαδικτυακό εργαλείο Exodus Privacy (Εικόνα 6.28) παρατηρείται ότι έχουν βρεθεί 2 ιχνηλάτες (trackers):

α) Google CrashLytics: Το Crashlytics προσφέρει μια ποικιλία υπηρεσιών για προγραμματιστές εφαρμογών, όπως:

   a. Λαμβάνει και αναλύει αναφορές σφαλμάτων εφαρμογών που μπορεί να περιέχουν δεδομένα για συγκεκριμένο χρήστη και συσκευή.

b. Εκτελεί αναλύσεις σε αρχεία καταγραφής εφαρμογών, ακόμα και την ακριβή γραμμή κώδικα στην οποία η εφαρμογή έχει πρόβλημα.

c. Εκτελεί αναλύσεις σε χρήστες εφαρμογών και χρησιμοποιεί διαφημίσεις στα μέσα κοινωνικής δικτύωσης. Εκτελεί ταυτότητα χρήστη μεταξύ συσκευών και έλεγχο ταυτότητας μέσω «Fabric»[18].

β) Google Firebase Analytics: Το Firebase προσφέρει λειτουργίες όπως αναλυτικά στοιχεία, βάσεις δεδομένων, ανταλλαγή μηνυμάτων και αναφορές σφαλμάτων[19].

Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 10 και είναι οι εξής:

1. Access_Network_State: προβολή συνδέσεων δικτύου
2. Access_Wifi_State: πλήρη πρόσβαση στο δίκτυο Wi-Fi
3. Download_Without_Notification: λήψη χωρίς ειδοποίηση
4. Foreground_Service: εκτέλεση υπηρεσίας σε πρώτο πλάνο
5. Internet: έχει πλήρη πρόσβαση στο δίκτυο
6. Receive_Boot_Completed: λειτουργία κατά την εκκίνηση
7. Wake_Lock: εμποδίζει το τηλέφωνο να βρίσκεται σε κατάσταση αναστολής
8. Write_External_Storage: τροποποιεί ή διαγράφει τα περιεχόμενα του κοινόχρηστου αποθηκευτικού χώρου
9. Receive: λαμβάνει αυτόματα περιεχόμενο στοιχείων
10. Bind_Get_Install_Referrer_Service: Σύνδεση Λήψη Εγκατάστασης

Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται 1 με επικίνδυνο δικαιώμα (high-risk permissions) της εφαρμογή OpenWHO, και αυτή είναι: Read_External_Storage, το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού με το δικαίωμα Read External Storage η εφαρμογή διαβάζει τον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό

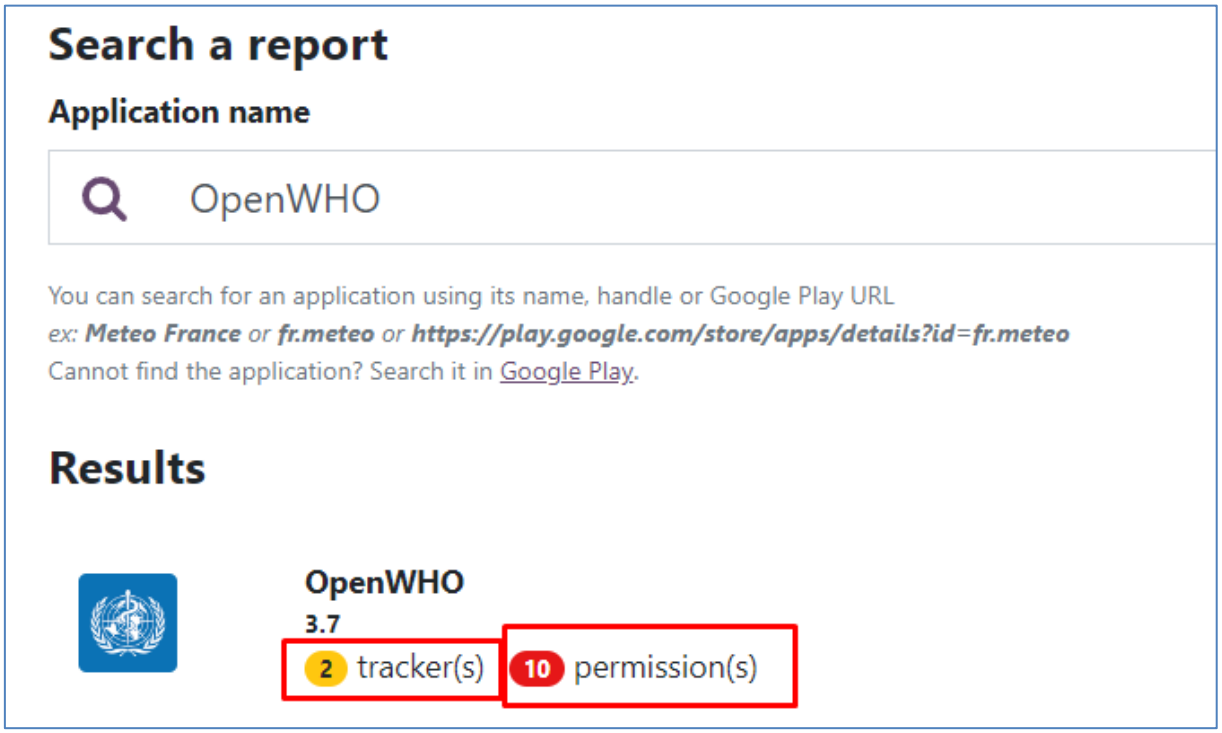
[18] Κιτ ανάπτυξης λογισμικού.

[19] Κανόνες ανίχνευσης:

- Κανόνας ανίχνευσης κώδικα: com.google.firebase.analytics. | com.google.android.gms.measurement. | com.google.firebase.firebase_analytics
- Κανόνας ανίχνευσης δικτύου: firebase\.com

υγείας). Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies).

Στην ιστοσελίδα: https://openwho.org/pages/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής openWHO δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής WHO Info: «Το openWHO αναλύει ανώνυμα σύνολα δεδομένων στο πλαίσιο έρευνας που στοχεύει στη βελτίωση της μαθησιακής σας εμπειρίας καθώς και των προσφορών μας» (openwho/Privacy and Data Protection, 2021)



Εικόνα 6.28: Έλεγχος της εφαρμογή OpenWHO με το διαδικτυακό εργαλείο Exodus Privacy.

Πηγή: *(exodus/OpenWHO, 2023)*.

Κεφάλαιο 7
Συμπεράσματα

Το διεθνές ρυθμιστικό πλαίσιο που χρησιμεύει για την προστασία του απορρήτου των προσωπικών δεδομένων ως ανθρώπινο δικαίωμα είναι ποικίλο, δεδομένων των προκλήσεων που αντιμετωπίζουν οι νομοθέτες για να συμβαδίσουν με την ταχέως εξελισσόμενη τεχνολογία.

Οι εφαρμογές υγείας για κινητά (m-Health) έχουν αποκτήσει δυναμική και επί του παρόντος είναι ευρέως διαδεδομένες στους χρήστες κινητών τηλεφώνων. Παρά το θερμό καλωσόρισμα από τους χρήστες, οι εφαρμογές m-health έχουν εγείρει ανησυχίες σχετικά με τη διαχείριση των προσωπικών τους πληροφοριών. Πράγματι, οι εφαρμογές m-health πρέπει να ασχολούνται με δεδομένα που σχετίζονται με την υγεία, τα οποία θεωρούνται πολύ ευαίσθητα και προστατεύονται σε μεγάλο βαθμό από εθνικούς και διεθνείς κανονισμούς όπως ο GDPR.

Οι εφαρμογές υγείας αποτελούν πλέον μέρος της παροχής υγειονομικής περίθαλψης. Έχουν τη δυνατότητα να αλλάξουν σημαντικά τη σχέση γιατρού-ασθενούς. Συγκεκριμένα, οι ασθενείς μπορούν να συμμετέχουν σημαντικά πιο ενεργά σε μεμονωμένα στάδια θεραπείας μέσω της χρήσης τέτοιων εφαρμογών.

Προτού τα προϊόντα τους είναι έτοιμα για την αγορά, οι κατασκευαστές και οι χειριστές προϊόντων υγείας πρέπει να συμμορφώνονται με πληθώρα νομικών προτύπων σε ένα περίπλοκο ρυθμιστικό περιβάλλον. Αυτά ενέχουν μεγάλη πιθανότητα σύγκρουσης και συνεπώς ευθύνης. Κεντρικής σημασίας - ιδίως όσον αφορά την αποδοχή των εφαρμογών υγείας από τους ασθενείς - είναι η συμμόρφωση με πολύπλοκες απαιτήσεις προστασίας δεδομένων και ασφάλειας δεδομένων. Εδώ, είναι σημαντικό να διασφαλιστεί η συμμόρφωση με τους ισχύοντες κανονισμούς και τις επίσημες απαιτήσεις με την εφαρμογή προσαρμοσμένων τεχνικών και οργανωτικών μέτρων.

Ωστόσο, με τη βοήθεια καλά μελετημένων εννοιών, ο κίνδυνος δυσάρεστων νομικών εκπλήξεων μπορεί να ελαχιστοποιηθεί.

Με στόχο να αξιολογηθεί η τρέχουσα κατάσταση πρακτικής στις εφαρμογές m-health σχετικά με την προστασία των δεδομένων που σχετίζονται με την υγεία, αναλύεται ένα αντιπροσωπευτικό σύνολο 10 εφαρμογών (Coronapas της Δανίας, Passe Covid της Πορτογαλίας, CovPass της Γερμανίας, CovScan Cyprus και CovPass Cyprus της Κυπριακής Κυβέρνησης, Covid Free GR και MyHealth της Ελληνικής Δημοκρατίας, COVID Alert NJ από το Υπουργείο Υγείας του Νιου Τζέρσεϋ (DOH), WHO Info και OpenWHO του Παγκόσμιου Οργανισμού Υγείας / ΠΟΥ), και μελετήθηκαν οι διάφορες πτυχές της ασφάλειας τους και οι πολιτικές και πρακτικές απορρήτου από την πλατφόρμα Google Play και με το διαδικτυακό εργαλείο Exodus Privacy.

Η παρούσα μελέτη υπογραμμίζει πολλές σημαντικές και δευτερεύουσες ελλείψεις των εφαρμογών m-health. Ένα μεγάλο μέρος των εφαρμογών που αξιολογήθηκαν διαπιστώθηκε ότι θα μπορούσαν να θέσουν σε κίνδυνο το απόρρητο και την ασφάλεια των χρηστών παραβιάζοντας τους ευαίσθητους κανονισμούς προστασίας δεδομένων που έχουν τεθεί για την πρόληψη της ακατάλληλης και ανεξέλεγκτης χρήσης, επεξεργασίας και αποκάλυψης δεδομένων υγείας σε τρίτους. Σύμφωνα με την παρούσα ανάλυση, ένας σχετικός αριθμός δημοφιλών εφαρμογών m-health θα μπορούσε να παραβιάσει το απόρρητο των χρηστών αποκαλύπτοντας ευαίσθητες πληροφορίες όπως καταστάσεις υγείας, ιατρικά συμπτώματα, φωτογραφίες, τοποθεσία, e-mail και κωδικούς πρόσβασης.

Δηλαδή κάποιες επεξεργασίες δεν είναι διαφανείς αφού υπάρχουν ιχνηλάτες χωρίς προηγούμενη σαφή ενημέρωση, αφού ζητούνται επικίνδυνα δικαιώματα χωρίς πλήρη τεκμηρίωση της αναγκαιότητάς τους.

Η έλλειψη κρυπτογράφησης, η χρήση του GET αντί των αιτημάτων POST για τη μετάδοση ευαίσθητων δεδομένων και οι ανασφαλείς πρακτικές προγραμματισμού, είναι μερικά από τα κύρια ανοιχτά ζητήματα ασφάλειας και απορρήτου που πρέπει να επιλύσουν οι προγραμματιστές κατά τη δημιουργία εφαρμογών m-health. Η δημιουργία προφίλ χρήστη, είτε για σκοπούς διαφήμισης και μάρκετινγκ είτε για παρακολούθηση της συμπεριφοράς των χρηστών, είναι μια πρόσθετη ανησυχία σχετικά με το απόρρητο που πρέπει να ληφθεί υπόψη για να διασφαλιστεί το απόρρητο των χρηστών. Παρόλο που η συμμόρφωση με τους ισχύοντες κανονισμούς προστασίας δεδομένων θα πρέπει να παρέχει στους χρήστες εφαρμογών m-health διαφάνεια δεδομένων, εξακολουθεί να είναι δύσκολο να επιτευχθεί λειτουργικότητα.

Πρέπει επίσης να σημειωθεί ότι στην ΕΕ, οποιαδήποτε πληροφορία τοποθεσίας ή οποιοδήποτε αναγνωριστικό συσκευής που δεσμεύει μοναδικά ένα μέρος ή μια συσκευή αντίστοιχα με ένα άτομο εμπίπτει στην κατηγορία προσωπικών δεδομένων. Ωστόσο, οι ΗΠΑ δεν έχουν ακόμη υιοθετήσει έναν ολοκληρωμένο νόμο περί απορρήτου των πληροφοριών, αλλά έχουν μάλλον περιορισμένους τομεακούς νόμους σε ορισμένους τομείς, όπως το HIPAA για την επεξεργασία δεδομένων που σχετίζονται με την υγεία. Άρα, δεν υπάρχει καθολικός ορισμός των προσωπικών δεδομένων σε όλα τα κράτη.

Εν συνεχεία παρουσιάζονται οι βαθμολογίες, οι αξιολογήσεις, οι ιχνηλάτες (trackers) και τα επικίνδυνα δικαιώματα (high-risk permissions) των κρατικών εφαρμογών υγείας Android ανά τον κόσμο:

1. Η εφαρμογή **Coronapas** - Τεστ COVID-19, αποτελεί Android εφαρμογή υγείας από το δημόσιο φορέα υγείας της Δανίας. Η Coronapas πληροί τις απαιτήσεις για το ψηφιακό πιστοποιητικό covid της ΕΕ. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Coronapas από τους 9190 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,6/5. Κατά τον έλεγχο της εφαρμογή Coronapas με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχει ιχνηλάτες (trackers) . Όσον αφορά τις άδειες / δικαιώματα έχει 9 (Access_Network_State, Camera, Flashlight, Internet, Use_Biometric, Use_Fingerprint, Vibrate, Wake_Lock, Decode) και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Coronapas, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Βεβαίως στην ιστοσελίδα: https://www.coronapass.org/privacy-policy/ όπου καταγράφονται τα privacy policy της εφαρμογής Coronapas δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής Coronapas: «*Η πολιτική απορρήτου μας βασίζεται στους όρους που χρησιμοποιεί ο Ευρωπαίος νομοθέτης για την υιοθέτηση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR*)».

2. Η εφαρμογή **Passe Covid** μπορεί να χρησιμοποιηθεί από οντότητες που πρέπει να επικυρώσουν τα ψηφιακά πιστοποιητικά Covid της ΕΕ, που εκδίδονται από όλα τα κράτη μέλη της ΕΕ, την Ισλανδία, το Λιχτενστάιν, τη Νορβηγία και την Ελβετία. Η εφαρμογή επικυρώνει την αυθεντικότητα του ψηφιακού πιστοποιητικού Covid της

ΕΕ και τη συμμόρφωση με τα πορτογαλικά κριτήρια επικύρωσης που ορίζονται από το DGS. Κατά τον έλεγχο της εφαρμογή Passe Covid με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι έχει βρεθεί 1 ιχνηλάτης (trackers) περιλαμβάνει Greystripe, εξατομικευμένο διαφημιστικό μάρκετινγκ, σε πλατφόρμα διαφήμισης για κινητά που αποκτήθηκε από την Conversant. Όσον αφορά τις άδειες / δικαιώματα έχει 4 (Access_Network_State, Camera, Flashlight, Internet), και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Passe Covid, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Ασφαλώς στην ιστοσελίδα: https://covidpass.eu/en/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής Passe Covid δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions) και ο ιχνηλάτης (trackers). Σύμφωνα με το τμήμα privacy policy της εφαρμογής Passe Covid: «*Τα δεδομένα σας δεν αποθηκεύονται πέρα από την ενεργή περίοδο λειτουργίας του προγράμματος περιήγησης και ο ιστότοπος δεν χρησιμοποιεί cookies.…Δεν αποστέλλονται δεδομένα σε τρίτους*)».

3. Η εφαρμογή **CovPass** μπορεί να χρησιμοποιηθεί για την αποθήκευση των ψηφιακών πιστοποιητικών COVID της ΕΕ από άλλα άτομα (π.χ. μέλη της οικογένειας) στα smartphone τους. Οι χρήστες της εφαρμογής αποφασίζουν πότε και σε ποιον θα εμφανίσουν τις πληροφορίες και τα δεδομένα τους. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass από τους 109000 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,6/5. Κατά τον έλεγχο της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχει βρεθεί ιχνηλάτης (trackers). Όσον αφορά τις άδειες / δικαιώματα έχει 4 (Access_Network_State, Camera, Foreground_Service, Internet) και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovPass, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Βέβαια στην ιστοσελίδα: https://www.digitaler-impfnachweis-app.de/en/data-privacy/ όπου καταγράφονται τα privacy policy της

εφαρμογής CovPass δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovPass: «*επονομαζόμενος υπεύθυνος επεξεργασίας που είναι υπεύθυνος για την επεξεργασία των προσωπικών σας δεδομένων σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων της ΕΕ (GDPR) και του Γερμανικού Ομοσπονδιακού Νόμου για την Προστασία Δεδομένων (BDSG)*».

4. Η επίσημη αίτηση της Κυπριακής Κυβέρνησης για την επαλήθευση της εγκυρότητας ενός Digital ψηφιακού Πιστοποιητικού COVID της ΕΕ (EUDCC) για οικιακή χρήση αποτελεί η εφαρμογή **CovScan** Cyprus. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovScan Cyprus από τους 637 περίπου αξιολογητές / χρήστες της, στην ιστοσελίδα Google Play είναι 1,2/5. Κατά τον έλεγχο της εφαρμογή CovScan με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι έχουν βρεθεί 2 ιχνηλάτες (trackers) (Microsoft Visual Studio App Center Analytics και Microsoft Visual Studio App Center Crashes). Όσον αφορά τις άδειες / δικαιώματα έχει 7 (Access_Network_State, Camera, Foreground_Service, Internet, Receive Boot Completed, Reorder Tasks, Wake Lock) και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovScan, το δικαίωμα «Camera» , το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Βέβαια στην ιστοσελίδα: https://wiki.eudcc.gov.cy/en/privacy.php/ όπου καταγράφονται τα privacy policy της εφαρμογής CovScan δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovScan: «*Η εφαρμογή «CovScan» έχει σχεδιαστεί για την εκτέλεση της επαλήθευσης/ελέγχου της γνησιότητας, εγκυρότητας και ακεραιότητας των ψηφιακών πιστοποιητικών Covid-19, εφεξής «η εφαρμογή», η οποία βασίζεται στο πλαίσιο της εφαρμογής του Κανονισμού. ΕΕ) 2021/953 και των Λοιμωδών Νοσημάτων (Καθορισμός Μέτρων για την Πρόληψη της Εξάπλωσης του Κορωνοϊού COVID-19 Διάταγμα του 2021) Διατάγματα, που εκδόθηκαν από τον Υπουργό Υγείας της Κυπριακής Δημοκρατίας*».

5. Η **CovPass** Cyprus αποτελεί την επίσημη εφαρμογή ηλεκτρονικού πορτοφολιού της Κυπριακής Κυβέρνησης όπου οι χρήστες μπορούν να σαρώσουν, να αποθηκεύσουν και να έχουν πρόσβαση στο Digital ψηφιακό πιστοποιητικό COVID της ΕΕ (EUDCC).

Ισχύει μόνο για χρήστες των οποίων το EUDCC εκδόθηκε στην Κύπρο και περιέχει κωδικό TAN (transaction authentication number). Οι βαθμολογίες και αξιολογήσεις της εφαρμογή CovPass Cyprus από τους 1120 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,4/5. Κατά τον έλεγχο της εφαρμογή CovPass με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers). Όσον αφορά τις άδειες / δικαιώματα έχει 8 (Access_Network_State, Camera, Foreground_Service, Internet, Receive Boot Completed, Use_Biometric, Use_Fingerprint, Wake Lock), και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή CovPass, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Αναμφίβολα στην ιστοσελίδα: https://wiki.eudcc.gov.cy/en/privacy.php/ όπου καταγράφονται τα privacy policy της εφαρμογής CovPass δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής CovPass: «*Η εφαρμογή «CovPass» που φιλοξενεί το ψηφιακό πιστοποιητικό Covid, εφεξής «η εφαρμογή» δημιουργήθηκε για την εφαρμογή του Κανονισμού (ΕΕ) 2021/953. Ο παρών κανονισμός προβλέπει την αμοιβαία αναγνώριση των πιστοποιητικών που εκδίδονται από τα κράτη μέλη της ΕΕ στους πολίτες για τη διευκόλυνση της ελεύθερης κυκλοφορίας τους μεταξύ κρατών μελών. Τα προσωπικά σας δεδομένα που καταχωρούνται σε αυτό θα υποβάλλονται σε επεξεργασία σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, εφεξής «GDPR» και της Προστασίας Φυσικών Προσώπων σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και την Ελεύθερη Διακίνηση Τέτοιου Δεδομένων Νόμου του 2018, Ν.125(Ι)/2018, εφεξής «η Εθνική Νομοθεσία», αμφότερα αποτελούν «το νομοθετικό πλαίσιο για την προστασία ή τα προσωπικά δεδομένα»*)».

6. Η εφαρμογή **Covid Free** GR αποτελεί την επίσημη ελληνική εφαρμογή για την επιβεβαίωση ευρωπαϊκών ψηφιακών πιστοποιητικών COVID και είναι διαθέσιμη μέσω του επίσημου λογαριασμού της Ελληνικής Δημοκρατίας. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή Covid Free GR από τους 4790 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 3,7/5. Κατά τον έλεγχο της εφαρμογή Covid Free GR με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχουν

βρεθεί ιχνηλάτες (trackers). Όσον αφορά τις άδειες / δικαιώματα έχει 3 (Access_Network_State, Camera, Internet), και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται ένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή Covid Free GR, το δικαίωμα «Camera», το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού η εφαρμογή «σκανάρει τα πιστοποιητικά υγείας. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Αναμφίβολα στην ιστοσελίδα: https://covidfree.gov.gr/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής Covid Free GR δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Ομόγνωμα με το τμήμα privacy policy της εφαρμογής Covid Free GR: «*Η Ανεξάρτητη Αρχή με την επωνυμία «ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ» (ΕΑΔ) υπό την ιδιότητά της ως Υπεύθυνης Επεξεργασίας των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας κατά τη λειτουργία της ειδικής ηλεκτρονικής εφαρμογής για τον έλεγχο της εγκυρότητας, της γνησιότητας και της ακεραιότητας του Ψηφιακού Πιστοποιητικού COVID -19 της Ε.Ε. (EU Digital COVID Certificate - EUDCC) και της βεβαίωσης εμβολιασμού της παρ. 5 του άρθρου 55 του ν. 4764/2020 (Α' 256) ή ισοδύναμου πιστοποιητικού ή βεβαίωσης, που φέρει το φυσικό́ πρόσωπο - κάτοχος, διά της σάρωσης του σχετικού κωδικού QR, με τη χρήση της ειδικής ηλεκτρονικής εφαρμογής CovidFreeGr, εγγυάται τον σεβασμό της ιδιωτικότητας των φυσικών προσώπων καθώς και την προστασία των προσωπικών τους δεδομένων».*

7. Η εφαρμογή MyHealth αποτελεί τον ηλεκτρονικό Ιατρικό Φάκελο Ασθενούς στην Ελλάδα. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή MyHealth από τους 3450 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,0/5. Κατά τον έλεγχο της εφαρμογή MyHealth με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers). Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 17 (Access_Network_State, Access_Wifi_State, Foreground_Service, Internet, Read_External_Storage, Receive_Boot_Completed, Request_Ignore_Battery_Optimizations, System_Alert_Window, Use_Biometric, Use_Fingerprint, Use_Full_Screen_Intent, Vibrate, Wake_Lock, Write_External_Storage, Write_Settings, Receive, Bind_Get_Install_Referrer_Service), Σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύονται 4 επικίνδυνα δικαιώματα (high-risk permissions) της εφαρμογή MyHealth, και αυτά είναι: Read_External_Storage, System_Alert_Window, Write_External_Storage,

Write_Settings, τα οποία σύμφωνα με την ερευνήτρια: το Read_External_Storage το οποίο διαβάζει τον Εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό υγείας), το Write External Storage με το οποίο η εφαρμογή έχει την δυνατότητα εγγραφής σε εξωτερική αποθηκευτική μονάδα του smartphone (προφανώς πιστοποιητικού υγείας), το Write Settings με το οποίο η εφαρμογή ρυθμίζει εγγραφή του εκάστοτε πιστοποιητικού υγείας στο smartphone και το System Alert Window το οποίο αποτελεί «παράθυρο» ειδοποίησης συστήματος για κάθε μεταβολή της εφαρμογής δεν αποτελούν απειλή σύμφωνα με τις παραπάνω διεργασίες που κατεγράφησαν. Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Βέβαια στην ιστοσελίδα: https://myhealth.gov.gr/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής MyHealth δεν αναφέρονται τα παραπάνω επικίνδυνα δικαιώματα, με την εξής δήλωση: «*Το Υπουργείο Υγείας υπό την ιδιότητά του ως Υπεύθυνος Επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας κατά τη λειτουργία της ειδικής ηλεκτρονικής εφαρμογής για κινητές συσκευές (mobile application) «myHealth» εγγυάται τον σεβασμό της ιδιωτικότητας των φυσικών προσώπων καθώς και την προστασία των προσωπικών τους δεδομένων*».

8. Η εφαρμογή **COVID Alert NJ** διατίθεται από το Υπουργείο Υγείας του Νιου Τζέρσεϋ (Department of Health / DOH) των ΗΠΑ για να συμπληρώσει την ολοκληρωμένη προσπάθεια ανίχνευσης επαφών COVID-19 του Νιου Τζέρσεϋ. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή COVID Alert NJ από τους 8980 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 4,3/5. Κατά τον έλεγχο της εφαρμογή COVID Alert NJ με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι δεν έχουν βρεθεί ιχνηλάτες (trackers). Όσον αφορά τις άδειες / δικαιώματα έχει 7 (Access_Network_State, Access_Wifi_State, Bluetooth, Foreground_Service, Internet, Receive_Boot_Completed, Vibrate) καο σύμφωνα με τα επίπεδα προστασίας της Google δεν υποδεικνύεται κανένα επικίνδυνο δικαίωμα (high-risk permissions) της εφαρμογή COVID Alert NJ.

9. Με την εφαρμογή **WHO Info**/World Health Organization, η οποία αποτελεί την επίσημη εφαρμογή πληροφοριών του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ - WHO / World Health Organization), ο εκάστοτε χρήστης έχει τις τελευταίες πληροφορίες για την υγεία στο τηλέφωνό του. Κατά τον έλεγχο της εφαρμογή WHO Info με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι έχει βρεθεί 1 ιχνηλάτης

(trackers), ο Google Firebase Analytics: Το Firebase προσφέρει λειτουργίες όπως αναλυτικά στοιχεία, βάσεις δεδομένων, ανταλλαγή μηνυμάτων και αναφορές σφαλμάτων. Ασφαλώς στην ιστοσελίδα: https://www.who.int/about/policies/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής WHO Info δεν αναφέρονται ο παραπάνω επικίνδυνος ιχνηλάτης. Σύμφωνα με το τμήμα privacy policy της εφαρμογής WHO Info: «*Οι πληροφορίες που συλλέγονται κατά τη γενική περιήγηση στον τομέα "who.int" χρησιμοποιούνται για την ανάλυση των τάσεων και της χρήσης του ιστότοπου του ΠΟΥ και για τη βελτίωση της χρησιμότητας του ιστότοπου. Δεν συνδέεται με καμία προσωπική πληροφορία …. Δεν πουλάμε ούτε κοινοποιούμε οποιεσδήποτε προσωπικές πληροφορίες που παρέχονται εθελοντικά στον ιστότοπο του ΠΟΥ σε κανένα τρίτο μέρος*». Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 9 και είναι οι εξής: (Access_Network_State, Access_Wifi_State, Read_Calendar, Read_External_Storage, Wake_Lock, Write_Calendar, Write_External_Storage, Receive, Bind_Get_Install_Referrer_Service), και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύονται 4 επικίνδυνα δικαιώματα (high-risk permissions) της εφαρμογή WHO Info, όπως τα: Read_Calendar, Read_External_Storage, Write_Calendar, Write_External_Storage, τα οποία σύμφωνα με την ερευνήτρια δεν αποτελούν απειλή διότι είναι απόλυτα αναμενόμενα αφού με το δικαίωμα Read Calendar η εφαρμογή διαβάζει την χρονική διάρκεια των πιστοποιητικών υγείας και ενημερώνεται για την λήξη αυτών, με το δικαίωμα Read External Storage η εφαρμογή διαβάζει τον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό υγείας), με το δικαίωμα Write Calendar η εφαρμογή γράφει την χρονική διάρκεια των πιστοποιητικών υγείας και ενημερώνεται για την λήξη αυτών, τέλος με το δικαίωμα Write External Storage γράφει στον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς πιστοποιητικό υγείας). Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Από το τμήμα privacy policy της εφαρμογής WHO Info δεν προκύπτει αναγκαιότητα των επικίνδυνων δικαιωμάτων (high-risk permissions) σύμφωνα με τα επίπεδα προστασίας της Google. Δηλαδή στην ιστοσελίδα: https://www.who.int/about/policies/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής WHO Info, εκτός των άλλων αναφέρονται: «*Οποιεσδήποτε πληροφορίες παρέχονται στον ΠΟΥ από χρήστες του ιστότοπου του ΠΟΥ τηρούνται με*

τη μέγιστη προσοχή και ασφάλεια και δεν θα χρησιμοποιηθούν με τρόπους διαφορετικούς από εκείνους που ορίζονται στην παρούσα πολιτική απορρήτου ή σε πολιτικές ειδικές για τον ιστότοπο ή με τρόπους που έχετε ρητά συναινέσει. Ο ΠΟΥ χρησιμοποιεί μια σειρά τεχνολογιών και μέτρων ασφαλείας για την προστασία των πληροφοριών που διατηρούνται στα συστήματά μας από απώλεια, κακή χρήση, μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη, τροποποίηση ή καταστροφή» (Privacy policy / WHO Info, 2021).

10. Η εφαρμογή **OpenWHO**: Knowledge for Health είναι η πλατφόρμα διαδραστικής μεταφοράς γνώσης της Παγκόσμιας Οργάνωσης Υγείας (WHO) που προσφέρει online μαθήματα για τη βελτίωση της ανταπόκρισης σε καταστάσεις έκτακτης ανάγκης για την υγεία. Οι βαθμολογίες και αξιολογήσεις της εφαρμογή OpenWHO από τους 4340 περίπου αξιολογητές / χρήστες της στην ιστοσελίδα Google Play είναι 2,6/5. Κατά τον έλεγχο της εφαρμογή OpenWHO με το διαδικτυακό εργαλείο Exodus Privacy παρατηρείται ότι έχουν βρεθεί 2 ιχνηλάτες (trackers): ο Google CrashLytics και ο Google Firebase Analytics. Όσον αφορά τις άδειες / δικαιώματα (permissions) έχει 10 (Access_Network_State, Access_Wifi_State, Download_Without_Notification, Foreground_Service, Internet, Receive_Boot_Completed, Wake_Lock, Write_External_Storage, Receive, Bind_Get_Install_Referrer_Service), και σύμφωνα με τα επίπεδα προστασίας της Google υποδεικνύεται 1 με επικίνδυνα δικαιώματα (high-risk permissions) της εφαρμογή OpenWHO, και αυτή είναι: Read_External_Storage, το οποίο σύμφωνα με την ερευνήτρια δεν αποτελεί απειλή διότι είναι απόλυτα αναμενόμενο αφού με το δικαίωμα Read External Storage η εφαρμογή διαβάζει τον εξωτερικό χώρο αποθήκευσης της συσκευής smartphone (προφανώς για πιστοποιητικό υγείας). Επιπλέον κάποια δικαιώματα όπως, τα παραπάνω, δεν προκύπτει με σαφήνεια η αναγκαιότητά τους με βάση τα κείμενα των πολιτικών απορρήτου (privacy policies). Στην ιστοσελίδα: https://openwho.org/pages/privacy/ όπου καταγράφονται τα privacy policy της εφαρμογής openWHO δεν αναφέρεται το παραπάνω επικίνδυνο δικαίωμα (high-risk permissions). Σύμφωνα με το τμήμα privacy policy της εφαρμογής WHO Info: «Το openWHO αναλύει ανώνυμα σύνολα δεδομένων στο πλαίσιο έρευνας που στοχεύει στη βελτίωση της μαθησιακής σας εμπειρίας καθώς και των προσφορών μας» (openwho/Privacy and Data Protection, 2021).

Υπό το πρίσμα των παραπάνω, ειδικοί σε θέματα ασφάλειας και υποστηρικτές της ιδιωτικής ζωής κηρύττουν τον κώδωνα του κινδύνου για πιθανές βλάβες στο απόρρητο

που προέρχονται από εφαρμογές m-health που επεξεργάζονται προσωπικά και ευαίσθητα δεδομένα και ζητούν κατάλληλα αντίμετρα. Όπως αποκαλύπτεται από την Πράσινη Βίβλο m-Health της Ευρωπαϊκής Επιτροπής του 2014, οι ευρωπαίοι πολίτες δεν εμπιστεύονται τις εφαρμογές m-Health καθώς το 67% του ερωτηθέντος πληθυσμού δήλωσε ότι δεν θα χρησιμοποιούσε ποτέ καμία δυνατότητα m-health του κινητού τους τηλεφώνου για την υποστήριξη των υγεία (European Union/mHealth, 2021). Σε μια προσπάθεια να χτίσει γερές βάσεις και εύκολα εφαρμόσιμα πρότυπα απορρήτου για την ανάπτυξη εφαρμογών m-health, και ειδικά για την ενίσχυση της εμπιστοσύνης μεταξύ των χρηστών τους, η Ευρωπαϊκή Επιτροπή εξέδωσε το 2016 ένα σχέδιο «Κώδικα Δεοντολογίας για το απόρρητο για κινητές εφαρμογές υγείας / Code of Conduct on privacy for mHealth apps», το οποίο υπόκειται στη συμμόρφωσή του με τις διατάξεις του GDPR, σύμφωνα με τα πρότυπα και τις αρχές προστασίας δεδομένων (European Union/Code of Conduct on privacy for mHealth apps, 2016). Βέβαια, ο εν λόγω κώδικας χρήζει αναθεώρησης εν όψει το νέου νομικού πλαισίου.

Λαμβάνοντας υπόψη τη νέα πρόταση Κανονισμού της ΕΕ για το διαμοιρασμό δεδομένων υγείας (European Health Data Space), καθίσταται κατά τη γνώμη σας σαφές ότι είναι απόλυτα αναγκαία η ανάπτυξη κατάλληλων προτύπων και τεχνολογιών, οι οποίες θα επιβάλλουν συγκεκριμένες απαιτήσεις τόσο στους αναλυτές όσο και στους σχεδιαστές «έξυπνων» εφαρμογών υγείας: οι αρχές της διαφάνειας και της προστασίας των δεδομένων από το σχεδιασμό πρέπει να ικανοποιούνται εγγενώς, με τρόπο που να μπορεί να αποδεικνύεται. Μόνο έτσι θα υπάρξει απόλυτος σεβασμός στο θεμελιώδες ατομικό δικαίωμα της ιδιωτικότητας και προστασίας προσωπικών δεδομένων, το οποίο με τη σειρά του θα ενισχύσει την εμπιστοσύνη των πολιτών στις εφαρμογές αυτές – μία παράμετρος κρίσιμη για την επιτυχή υιοθέτησή τους και την επίτευξη των σκοπών τους.

Εν κατακλείδι, συμπεραίνεται ότι οι πολιτικές απορρήτου θα πρέπει να είναι απόλυτα ξεκάθαρες, να μην αφήνουν αμφιβολίες ως προς τι επεξεργασία δεδομένων γίνεται (η οποία θα πρέπει να σέβεται τις αρχές «data protection by design» και «by default»), ενώ ιδανικά θα πρέπει να υπάρχει εξήγηση για κάθε δικαίωμα υψηλού κινδύνου που η εφαρμογή απαιτεί.

Βιβλιογραφία

128th Session of the Committee of Ministers. (2018, 5 17-18). *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.* Ανάκτηση 12 2022, από Council of Europe Portal: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

Adiyasa, R. P., & Wirata, R. B. (2023, March). Determinants of BECA (breasts examination for cancer awareness) mobile application use. *Enfermería Clínica, 33*(1), σσ. S1-S6.

Ahn, H., & Park, E. (2022, May). Determinants of consumer acceptance of mobile healthcare devices: An application of the concepts of technology acceptance and coolness. *Telematics and Informatics, 70*.

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2021, September). Women's mHealth Apps: Scoping Review and Content Analysis of Privacy, Data Sharing, and Data Security Policies. *JMIR mHealth and uHealth*.

Amer, E., & El-Sappagh, S. (2022, May). Robust deep learning early alarm prediction model based on the behavioural smell for android malware. *Computers & Security, 116*.

AVG / App Permissions on Android. (2023). *App Permissions on Android & How to Control Them*. Ανάκτηση 3 2023, από AVG Signal Blog: https://www.avg.com/en/signal/guide-to-android-app-permissions-how-to-use-them-smartly#:~:text=It%27s%20the%20%E2%80%9Cdangerous%E2%80%9D%20permissions%20that,have%20the%20potential%20for%20misuse

Bhatt, B. N., & Furia, C. A. (2022, October). Automated repair of resource leaks in Android applications. *Journal of Systems and Software, 192*.

Britannica/Android operating system. (2022, 8 23). *Android operating system.* Ανάκτηση 12 2022, από Encyclopedia Britannica: https://www.britannica.com/technology/Android-operating-system

Callaham, J. (2022, 8 13). *The history of Android: The evolution of the biggest mobile OS in the world.* Ανάκτηση 12 2022, από Authority: https://www.androidauthority.com/history-android-os-name-789433/

Consolidated version of the Treaty on European Union. (2012, 10 26). Ανάκτηση 12 2022, από European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

Coronapas - COVID-19 test. (2020). Ανάκτηση 3 2023, από www.sundhed.dk: https://www.sundhed.dk/borger/min-side/corona/covidpas/

Coronapas. (2020). Ανάκτηση 3 2023, από Google Play: https://play.google.com/store/apps/details?id=dk.sum.ssicpas&hl=el&gl=DK&pli=1

coronapass/privacy policy. (2021). *coronapass*. Ανάκτηση 5 2023, από privacy policy: https://www.coronapass.org/privacy-policy

COVID Alert NJ. (2020, 9 18). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=com.nj.gov.covidalert&hl=el&gl=US

Covid Free GR /privacy policy. (2021). *Covid Free GR*. Ανάκτηση 5 2023, από privacy policy: https://covidfree.gov.gr/privacy/

Covid Free GR Wallet/Hellenic Republic. (2021). Ανάκτηση 3 2023, από Google Play: https://play.google.com/store/apps/details?id=gr.gov.dcc.wallet&hl=el&gl=US

CovPass / privacy policy. (2021). *CovPass*. Ανάκτηση 5 2023, από privacy policy: https://wiki.eudcc.gov.cy/en/privacy.php

CovPass. (2021, 10 5). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=de.rki.covpass.app&hl=el&gl=US

CovPass Cyprus. (2021, 8 29). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=cy.gov.eudcc.app.wallet.android&hl=el&gl=US

CovPass RKI / privacy policy. (2021). *CovPass RKI*. Ανάκτηση 5 2023, από privacy policy: https://www.digitaler-impfnachweis-app.de/en/data-privacy/

CovScan Cyprus. (2021, 7 21). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=cy.gov.eudcc.app.verifier_lite.android&hl=el&gl=US

Elprocus/Android Operating System & Its Features. (2022). *Android Operating System & Its Features*. Ανάκτηση 1 2023, από Elprocus: https://www.elprocus.com/what-is-android-introduction-features-applications/

European Commission/Privacy code of conduct on mobile health apps. (2021). *Privacy code of conduct on mobile health apps*. Ανάκτηση 3 2023, από European Commission: https://digital-strategy.ec.europa.eu/en/policies/privacy-mobile-health-apps

European Convention on Human Rights. (2021). Ανάκτηση 12 1, από Council of Europe: https://www.echr.coe.int/Documents/Convention_ENG.pdf

European Union/Code of Conduct on privacy for mHealth apps. (2016, June 7). *Code of Conduct on privacy for mHealth apps*. Ανάκτηση 4 2023, από European Union: https://digital-strategy.ec.europa.eu/en/library/code-conduct-privacy-mhealth-apps-has-been-finalised

European Union/EDPB-EDPS. (2022, 3). *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*. Ανάκτηση 2 2023, από European Union: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en

European Union/mHealth. (2021, March 9). *Green Paper on mobile health ("mHealth")*. Ανάκτηση 4 2023, από European Union: https://digital-strategy.ec.europa.eu/en/library/green-paper-mobile-health-mhealth

exodus/COVID Alert NJ. (2023, 4). *COVID Alert NJ*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/com.nj.gov.covidalert/latest/

exodus/Covid Free GR. (2023, 4). *Covid Free GR*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/gr.gov.dcc.mini/latest/#permissions

exodus/CovScan Cyprus. (2023, 4). *CovScan Cyprus*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/cy.gov.eudcc.app.verifier_lite.android/latest/#trackers

exodus/MyHealth. (2023, 4). *MyHealth*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/gr.gov.myhealth/latest/#permissions

exodus/OpenWHO. (2023, 4). *OpenWHO*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/de.xikolo.openwho/latest/#trackers

exodus/WHO Info. (2023, 4). *WHO Info*. Ανάκτηση από exodus-privacy.eu.org: https://reports.exodus-privacy.eu.org/el/reports/org.who.infoapp/latest/#trackers

Fan, M., Yuy, L., Chenz, S., Zhouy, H., Luoy, X., Li, S., . . . Liu, J. (2020, August). An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps. *IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*.

Galetsi, P., Katsaliaki, K., & Kumar, S. (2023, March). Exploring benefits and ethical challenges in the rise of mHealth (mobile healthcare) technology for the common good: An analysis of mobile applications for health specialists. *Technovation, 121*.

GDPR / Personal Data. (2020). Ανάκτηση από consulting company : https://gdpr-info.eu/issues/personal-data/

Google Play / MyHealth. (2022). *MyHealth/Hellenic Republic*. Ανάκτηση 4 2023, από Google Play: https://play.google.com/store/apps/details?id=gr.gov.myhealth&hl=el

Guerra-Manzanares, A., Luckner, M., & Bahsi, H. (2022, September). Concept drift and cross-device behavior: Challenges and implications for effective android malware detection. *Computers & Security, 120*.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (1996). Ανάκτηση 3 2023, από Public Health Professionals Gateway: https://www.cdc.gov/phlp/publications/topic/hipaa.html

Hussain, M., Al-Haiqi, A., Zaidan, B., Zaidan, A., Kiah, M., Iqbal, S., . . . Abdulnabi, M. (2018, June). A security framework for mHealth apps on Android platform. *Computers & Security, 75*, σσ. 191-217.

Intersoft consulting/Άρθρο 14 GDPR. (2016). *Information to be provided where personal data have not been obtained from the data subject*. Ανάκτηση 3 2023, από Intersoft consulting: https://gdpr-info.eu/art-14-gdpr/

IntersoftGeneral/Άρθρο 13: GDPR. (2016). *Information to be provided where personal data are collected from the data subject*. Ανάκτηση 3 2023, από IntersoftGeneral/Data Protection Regulation: https://gdpr-info.eu/art-13-gdpr/

Kong, K., Zhang, Z., Guo, C., Han, J., & Long, G. (2022, December). PMMSA: Security analysis system for android wearable applications based on permission matching and malware similarity analysis. *Future Generation Computer Systems, 137*, σσ. 349-362.

Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023, July). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems, 144*, σσ. 271-290.

Machado, C., Cunha, A., & Jorge Gouveia, A. (2023). Migration of a stock management application in the healthcare industry to a Web/Mobile environment: a project report. *Procedia Computer Science, 2019*, σσ. 184-192.

Mazuera-Rozo, A., Escobar-Velásquez, C., Espitia-Acero, J., Vega-Guzmán, D., Trubiani, C., Linares-Vásquez, M., & Bavota, G. (2022, May). Taxonomy of security weaknesses in Java and Kotlin Android apps. *Journal of Systems and Software, 187*.

Mia, R., Shahriar, H., Valero, M., Sakib, N., Saha, B., & Barek, A. (2022, December). A comparative study on HIPAA technical safeguards assessment of android mHealth applications. *Smart Health, 26*.

mobile application) «myHealth». (2021). Ανάκτηση 5 2023, από www.dpa.gr: https://myhealth.gov.gr/privacy/

Mulder, T., & Tudorica, M. (2020). Privacy Policies, Cross-border Health Data and the GDPR. *University of Groningen Faculty of Law Research Paper, 18*.

OECD/Tracking and tracing COVID. (2020, April 23). *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. Ανάκτηση 3 2023, από Organisation for EconomicCo-operation and Development: https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

Official Journal of the European Union. (2012, 10 26). Ανάκτηση 12 2022, από European Union: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:12012P/TXT

openwho/Privacy and Data Protection. (2021). Ανάκτηση 5 2023, από openwho.org: https://openwho.org/pages/privacy

OpenWHO: Knowledge for Health. (2022, 12 22). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=de.xikolo.openwho

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018, January). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access*.

Passe Covid / privacy policy. (2021). *Passe Covid*. Ανάκτηση 5 2023, από privacy policy: https://www.google.com/search?q=Passe+Covid+privacy+policy&sxsrf=APwXEdeajcvbDLVoF8jki8Jd0WNwYqLZ_w%3A1683265233667&ei=0ZZUZOWcKNSVxc8P3u-qgAU&ved=0ahUKEwilycLSu93-AhXUSvEDHd63ClAQ4dUDCA8&uact=5&oq=Passe+Covid+privacy+policy&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAzI

Passe Covid. (2021, 8 2). Ανάκτηση 3 2023, από Google Play: https://play.google.com/store/apps/details?id=pt.incm.eudcc.app.lite&hl=el&gl=US

PEPP-PT/mhealth-hub. (2020). *Pan-European Privacy-Preserving Proximity Tracing*. Ανάκτηση 3 2023, από mhealth-hub: https://mhealth-hub.org/pan-european-privacy-preserving-proximity-tracing

Perkins, S. (2023). *16 underrated Android 13 features you need to try*. Ανάκτηση 1 2023, από www.androidpolice.com: https://www.androidpolice.com/top-underrated-android-13-features/

Privacy by Design. (2016). Ανάκτηση 3 2023, από intersoft consulting: https://gdpr-info.eu/issues/privacy-by-design/

Privacy policy / WHO Info. (2021). Ανάκτηση 5 2023, από www.who.int: https://www.who.int/about/policies/privacy

Republic of Cyprus/Law 125(I)2018. (2018). *Office of the Commissioner for Personal Data Protection*. Ανάκτηση 12 2022, από Republic of Cyprus: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/2B53605103DCE4A4C225826300362211

Skyfii /Smartphone tracking. (2020, July 16). *Smartphone tracking*. Ανάκτηση 5 2023, από Skyfii Limited: https://skyfii.io/blog/smartphone-tracking-what-you-need-to-know

Tang, J., Li, R., Jiang, Y., Gu, X., & Li, Y. (2022, April). Android malware obfuscation variants detection method based on multi-granularity opcode features. *Future Generation Computer Systems, 129*, σσ. 141-151.

The Institution of ASEP and its Contribution to Public Administration. (2022). Ανάκτηση 12 2022, από ΑΣΕΠ: https://www.asep.gr/webcenter/portal/asep/SUPREME+COUNCIL+FOR+CIVIL+PERSONNEL+SELECTION+(ASEP)?_adf.ctrl-state=ara4bwj61_1&_afrLoop=13530923299986511 3#!%40%40%3F_afrLoop%3D13530923299986511 3%26_adf.ctrl-state%3Dara4bwj61_5

The National Council for Radio and Television (NCRTV). (2022). Ανάκτηση 12 2022, από Εθνικό Συμβούλιο Ραδιοτηλεόρασης (Ε.Σ.Ρ.): https://www.esr.gr/information/

TraceTogether. (2020, 3 9). Ανάκτηση 3 2023, από A Singapore Government Agency Website: https://www.tracetogether.gov.sg/

Treaty Office No.108. (1985, 10 1). Ανάκτηση 12 2022, από Council of Europe Portal: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

WHO Info. (2020, 4 13). Ανάκτηση 3 2023, από googlePlay: https://play.google.com/store/apps/details?id=org.who.infoapp

ΑΔΑΕ/Ρυθμιστικό Πλαίσιο. (2003). Ανάκτηση 12 2022, από Ελληνική Αρχή Ασφάλειας Επικοινωνιών και Απορρήτου: http://www.adae.gr/en/regulatory-framework/

Ευρωπαϊκή Επιτροπή/COM(2018). (2018, 6 5). *COM(2018).* Ανάκτηση 12 2022, από Ευρωπαϊκή Επιτροπή: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018PC0451&from=en

Ευρωπαϊκή Επιτροπή/Προστασία δεδομένων στην ΕΕ. (2016). *Προστασία δεδομένων στην ΕΕ*. Ανάκτηση 12 2022, από Ευρωπαϊκή Επιτροπή: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_el

Intersoft consulting/Άρθρο 25: GDPR. (2016). *Data protection by design and by default*. Ανάκτηση 3 2023, από Intersoft consulting: https://gdpr-info.eu/art-25-gdpr/

Ν. 2472/1997. (2019). Ανάκτηση 12 2022, από kodiko.gr: https://www.kodiko.gr/nomothesia/document/208063/nomos-2472-1997

Ν. 3471/2006. (2006). Ανάκτηση 12 2022, από kodiko.gr: https://www.kodiko.gr/nomothesia/document/155678/nomos-3471-2006

Ν. 4624/2019. (2022). Ανάκτηση 12 2022, από kodiko.gr: https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019

Νεοκλέους, Α. (2022). *Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) («GDPR») στην Κύπρο*. Ανάκτηση 12 2022, από OneTrust, LLC.: https://www.dataguidance.com/notes/cyprus-data-protection-overview

Οδηγία (ΕΕ) 2016/680. (2016, 5 4). Ανάκτηση 12 2022, από Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωση: https://www.dpa.gr/sites/default/files/2020-05/CELEX_32016L0680_EL_TXT.pdf

Συνήγορος του Πολίτη. (2022). Ανάκτηση 12 2022, από Συνήγορος του Πολίτη: https://www.synigoros.gr/el/category/synhgoros-toy-polith