Legal Feasibility
(νομικά ζητήματα)

Η εφαρμογή μας θα διαχειρίζεται προσωπικά δεδομένα χρηστών, αν και εφόσον ο χρήστης επιτρέπει την χρήση τους. Ο χειρισμός αυτών θα πρέπει να γίνεται με ιδιαίτερη προσοχή, ώστε να μην είναι προσβάσιμα από επιθέσεις ανταγωνιστών. Διαφορετικά, δημιουργείται ο κίνδυνος να οδηγηθούμε σε δικαστική διαμάχη με τους πελάτες μας, είτε αυτοί αποτελούν ένα κατάστημα που επέλεξε την πλατφόρμα μας, είτε αυτοί είναι απλοί χρήστες που χρησιμοποιούν την εφαρμογή μας για τις παραγγελίες τους. Τέτοιου είδους διαμάχες έχουν σοβαρό οικονομικό και χρονικό αντίκτυπο στο έργο μας, αλλά ταυτόχρονα πλήττουν την φήμη της επιχείρησής μας.

Σημαντικός για την λύση των παραπάνω πιθανών προβλημάτων είναι ο ρόλος του security lead που θα έχει ανατεθεί στους backend και mobile developers της εφαρμογής μας. Αυτοί θα είναι υπεύθυνοι για την εξέταση ασφάλειας σε κάθε στάδιο ανάπτυξης της εφαρμογής. Ο ρόλος τους έγκειται σε 5 βασικές κατηγορίες:

-Έλεγχος δεδομένων που συλλέγονται και διατηρούνται: Θα λαμβάνουν αποφάσεις για τα χρονικά διαστήματα που θα διατηρούνται δεδομένα χρηστών στο σύστημα και για το ποια θα είναι αυτά.

-Προσαρμογή κώδικα μεταξύ πλατφορμών για κινητές συσκευές: Κάθε λειτουργικό σύστημα κινητής τηλεφωνίας χρησιμοποιεί διαφορετική διεπαφή προγραμματισμού εφαρμογών (API), η οποία περιλαμβάνει διαφορετικές λειτουργίες ασφάλειας και χειρισμού αδειών. Επομένως, ο κώδικας θα πρέπει να προσαρμόζεται αναλόγως για κάθε ένα ξεχωριστά.

-Δημιουργία ασφαλών διαπιστευτηρίων χρήστη: Η εφαρμογή μας απαιτεί από τους χρήστες να δημιουργούν usernames και κωδικούς πρόσβασης. Η φύση της εφαρμογής μας απαιτεί υψηλό επίπεδο ελέγχου ταυτότητας (για παράδειγμα, υψηλές απαιτήσεις ισχύος κωδικού πρόσβασης) καθώς στον εκάστοτε λογαριασμό χρήστη θα υπάρχουν προσωπικές πληροφορίες όπως πληροφορίες πληρωμών και διευθύνσεις. Οι κωδικοί πρόσβασης χρηστών δεν θα πρέπει επίσης να αποθηκεύονται ως απλά κείμενα στον διακομιστή. Θα πρέπει να χρησιμοποιείται μια επαναλαμβανόμενη κρυπτογραφική συνάρτηση κατακερματισμού για να κατακερματίζονται οι κωδικοί πρόσβασης των χρηστών και στην συνέχεια, να επαληθεύονται με αυτές τις τιμές κατακερματισμού. Οι χρήστες θα μπορούν απλώς να επαναφέρουν τους κωδικούς πρόσβασής του αν τους ξεχάσουν.

-Κρυπτογράφηση δεδομένων: Οι security leads οφείλουν να χρησιμοποιήσουν transit encryption (SSL/TLS σε μορφή HTTPS) για την ασφάλιση προσωπικών δεδομένων και κλειδιών API κατά την μεταφορά αυτών από μια συσκευή στον διακομιστή μας. Αυτό είναι ιδιαίτερα σοβαρό επειδή πολλοί χρήστες χρησιμοποιούν μη ασφαλή δημόσια δίκτυα WiFi για πρόσβαση σε εφαρμογές. Με τη χρήση HTTPS, απαιτείται ένα ψηφιακό πιστοποιητικό από αξιόπιστο προμηθευτή (που μπορεί να βρεθεί σε πολύ χαμηλό κόστος) ώστε η εφαρμογή να το ελέγχει σωστά.

-Συνεχής έλεγχος ασφαλείας ακόμα και μετά την κυκλοφορία της εφαρμογής: Με την εφαρμογή διαθέσιμη για λήψη, οι security leads θα πρέπει να συνεχίζουν να ασχολούνται με την ασφάλεια της: ενημερώνοντας βιβλιοθήκες ασφαλείας, προωθώντας ενημερώσεις στους χρήστες και χρησιμοποιώντας τα σχόλια χρηστών για να εντοπίσουν και να διορθώσουν πιθανές ευπάθειες.

Τέλος, η σύσταση ομάδας με έμπειρους νομικούς που θα ασχολείται με θέματα εχεμύθειας και κατοχύρωσης πνευματικών δικαιωμάτων θα αποτελέσει την δικλείδα ασφαλείας στην αντιμετώπιση των νομικών ζητημάτων.