סקירת פרטיות ואבטחה – המגן 2

סקירה זו נועדה לבחון את היבטי הפרטיות ואבטחת המידע ביישומון "המגן 2" ולוודא כי הם תואמים את המוצהר על-ידי משרד הבריאות. הסקירה כוללת היבטים משפטיים וטכנולוגיים.

<u>רקע</u>

בעקבות התפשטות מגפת הקורונה בעולם, קם הצורך בהסתייעות באמצעים טכנולוגיים ככלי משלים למערך החקירות האפידמיולוגיות. במרץ 2020 השיק משרד הבריאות את יישומון "המגן 1" אשר אפשר להצליב נתוני מיקום (GPS) שנשמרו מקומית בטלפון הנייד של המשתמש, אל מול מקומות בהם שהו חולי קורונה מאומתים. ברגע שהיישומון זיהה חפיפה בין המיקומים שנשמרו בטלפון הנייד לבין מיקום של חולה מאומת, הוא התריע למשתמש על האפשרות כי נחשף לחולה קורונה והותיר בידיו את שיקול הדעת והבחירה האם להיכנס לבידוד ולדווח על כך למשרד הבריאות.

ביום 1.7.2020 עיגנה הכנסת בחוק הסמכת שירות הביטחון הכללי לסייע במאמץ הלאומי לצמצום התפשטות נגיף הקורונה החדש (הוראת שעה), התש"ף–2020 את הסמכת השב"כ להפעיל כלי מעקב לצורך סיוע במאבק בקורונה ("חוק איכוני השב"כ"). חוק איכוני השב"כ עודכן ב-20.7.2020 כך שמלבד ההסמכה למעקב אחר אזרחים, נקבע בו שמשרד הבריאות יעמיד לרשות הציבור טכנולוגיה אזרחית לאיתור מגעים קרובים עם חולים לשם צמצום התפשטות המגיפה.

לאחר החקיקה השיק משרד הבריאות את "המגן 2", המאפשר איתור מגע קרוב עם חולה, באמצעות טכנולוגיית בלוטות' (Bluetooth), זאת בנוסף להצלבת נתוני מיקום שהתאפשרה ב"המגן 1".

<u>סקירה טכנולוגית של היישומון</u>

"המגן 2" פועל בשתי דרכים: בדרך הראשונה, היישומון מזהה מיקום בעזרת GPS ו-Wifi Positioning. זיהוי מיקום מתבצע מאליו, בלא צורך בתקשורת עם מכשיר טלפון אחר שבו מותקן היישומון. יכולת זו קיימת כבר ב"המגן 1". בדרך השניה, היישומון מנטר קירבה בין שני מכשירים ניידים שבהם היישומון מותקן באמצעות Bluetooth Low Energy. יכולת זו התווספה ב"המגן 2". היא מאפשרת להיוודע אם אנשים שהו במרחק מטרים בודדים עד עשרות מטרים זה מזה לפרק זמן ממושך שדי בו לסכן אחד מהם בהדבקה אם השני יתברר לימים כחולה. הטלפונים מעבירים זה לזה איתותים ב-Bluetooth, ועל פי עוצמת האיתות מחשב היישומון את המרחק של הטלפונים זה מזה. בדרך זו היישומון יכול לפעול ביעילות גם בתוך מבנים, חללים סגורים או בתוך תחבורה ציבורית - בהם מתרחשות רבות מההדבקות. בגלל המגבלות של מערכות ההפעלה Android ו-iOS, שאינן מאפשרות ליישומונים לשדר למכשירים אחרים בעזרת Bluetooth כשהם פועלים ברקע, יתכן שהיעילות וצריכת הסוללה של Bluetooth צריכות להיבדק בתנאי אמת. חברת גוגל ואפל, מפתחות מערכת ההפעלה אנדרואיד ו-iOS פיתחו פרוטוקול המאפשר ליישומונים רשמיים של רשויות בריאות להשתמש ב-Bluetooth בעודן פועלות ברקע, אך ללא שימוש מקביל בשירותי מיקום. מסיבה זו, ממשרד הבריאות בחר שלא לבסס את "המגן 2" על פרוטוקול זה.

היישומון שומר מידע לגבי המיקומים או המגעים באופן מקומי בלבד, בטלפון של המשתמשים. איתותי Bluetooth בין טלפונים מוצפנים שמונעים מצב בו גורם ריכוזי יכול ללמוד על מגעים בין משתמשים. כאשר מגיעה רשימה של מיקומים וזמנים בהם היה חולה קורונה מאומת, ההתאמה בין המיקומים לבין הודעות ה-

Bluetooth מתבצעת מקומית בטלפון של המשתמש. לפיכך, אם נמצא מגע עם חולה מאומת, המשתמש הוא היחידי שיודע על כך, ויש לסמוך עליו כי יודיע למשרד הבריאות וייכנס לבידוד. "המגן 2" משתמש בנתוני המיקום כדי להגן על "המגן 2" מפני התקפות שמטרתן לגרום לזיהוי שגוי של מגעים, בעזרת התאמה בין נתוני ה-bluetooth והמיקום.

בנוסף, לפי משרד הבריאות, "המגן 2" מכיל יכולת לשחזור מסלולי תנועה של אדם שזוהה כחולה מאומת, במידה שהמשתמש בוחר לחלוק את המידע עם משרד הבריאות. אופציה זו מאפשרת תחקור אפידמיולוגי יעיל יותר, ומופעלת על ידי שליחת SMS למכשיר, והסכמה של המשתמשים לשיתוף המידע. נבהיר, כי בהיעדר בדיקה מול חולה מאומת, אין ברשותנו יכולת לבדוק נושא זה.

לשם בדיקת רמת האבטחה של היישומון, חטיבת הגנת הפרטיות וצוות התקיפה של מרכז הגנת הסייבר ב-BDO ישראל ערכה בדיקה טכנית ליישומון. הצוותים בחנו שלושה היבטים עיקריים:

1. האם מתבצעת העברת מידע מהיישומון לצדדים שלישיים;
2. האם המידע שהיישומון אוסף נשמרים בצורה מאובטחת ומוצפנת;
3. אלו הרשאות היישומון מבקש וכיצד נעשה שימוש בהרשאות אלו (לדוגמה: גישה לאנשי קשר, גלריית תמונות וכיו"ב).

הבדיקה וממצאיה הועברו למשרד הבריאות לעיון ותיקון. תקציר הבדיקה מצורף כנספח לסקירה זו.

<u>ניתוח היבטי הפרטיות</u>

שתי גרסאות יישומון המגן פותחו בהתאם לגישה של "הנדסת פרטיות" – Privacy by Design. גישה זו מבקשת להטמיע את הגנת הפרטיות במערכת מלכתחילה, כבר בשלב תכנון הטכנולוגיה, ולא רק בדיעבד. זו גישה ראויה ונבונה, ואנו מברכים עליה. פיתוח "המגן 2" לווה על ידי הרשות להגנת הפרטיות.

היישומון משקף כמה היבטים מרכזיים שהם עקרונות יסוד בדיני הגנת המידע האישי (Data Protection):

- **הסכמה מדעת**: השימוש ביישומון וולונטרי לחלוטין, וכפוף לבחירה של המשתמשים; תנאי השימוש מופיעים בכמה שפות, והם קצרים למדי ובהירים - בוודאי בהשוואה למקובל בהקשרים מסחריים; כל אלה מאפשרים למשתמשים לקבל החלטה מושכלת לגבי השימוש ביישומון. בנוסף, כל גישה של היישומון לנתונים בטלפון, דוגמת נתוני מיקום ובלוטות', דורשים אישור אקטיבי של המשתמש.
- **שליטת המשתמש במידע**: המידע שנאסף לגבי המיקום ולגבי האיתותים ממכשירים אחרים נשמר אך ורק ביישומון של המשתמש עצמו, ולא עובר למשרד הבריאות, למשתמשים האחרים או לאף גורם אחר. המידע נשמר במכשיר האישי של המשתמש. כל העברת מידע מתבצעת רק באופן אקטיבי על ידי המשתמש.
- **מחיקת המידע**: שליטת המשתמש במידע מתחזקת בכך שיש אפשרות פשוטה להסיר את היישומון - כמו כל הסרה של יישומון אחר, ולמחוק את המידע שהצטבר.
- **העברת מידע למשרד הבריאות**: קיימת אפשרות טכנית כזו אולם היא הופכת רלוונטית רק כאשר האדם אובחן כחולה, ובמסגרת החקירה האפידמיולוגית. גם במקרה כזה, ההחלטה אם לשתף את המידע עם משרד הבריאות תלויה אך ורק ברצונו של המשתמש.
- **מיזעור מידע**: היישומון אוסף רק מידע על מיקום ועל הקירבה למשתמשים אחרים, ואינו אוסף מידע עודף. איסוף המידע המינימלי שדרוש לשם מימוש התכלית של היישומון - איתור מגעים - חשובה עד

מאוד: היא מבטיחה שההסכמה ניתנת עבור מטרה מוגדרת, היא מצמצמת את הסיכון לזליגת שימושים ובכך משקפת את "עקרון צמידות המטרה", שלפיו מידע שנאסף למטרה מסוימת, צריך לשמש רק לאותה מטרה. בנוסף, ככל שנאסף פחות מידע, החשש מדליפת מידע מתוך המערכת או מפריצה מבחוץ - קטנים.

- **קוד פתוח**: משרד הבריאות שיחרר את קוד המקור של היישומון תחת רישיון מסוג MIT. הקוד זמין באתר **GitHub**. העובדה שהקוד של היישומון פתוח ונגיש לבקרה ציבורית חשובה. בכך מושגת שקיפות ומתאפשרת בקרה חיצונית אובייקטיבית של מומחי מחשבים, היכולים לוודא שההצהרות של משרד הבריאות בדבר שמירה מקומית של המידע, אי-העברתו, אפשרות מחיקתו וכדומה - אכן נכונות. שקיפות ובקרה כזו מעודדים את אמון הציבור במערכת.
- **הצפנה וסודיות**: איתותי Bluetooth ונתונים אחרים נשמרים באופן מוצפן. רק לטלפונים של המשתמשים יש מפתח שמאפשר קריאה של הנתונים. כך, גם אם המידע בטלפון ייחשף, לא ניתן יהיה להסיק מכך עם מי המשתמש היה במגע.

עם זאת, אנו ממליצים להוסיף רבדים נוספים להגנה על פרטיות המשתמשים -

- על משרד הבריאות לפרסם "תסקיר הגנת פרטיות", שמפרט את היבטי הפרטיות ביישומון. מסמך כזה חשוב כדי להנחות את הפיתוחים העתידיים של היישומון, וכדי לשמש מודל למצבים אחרים של "הנדסת פרטיות".
- בדומה להליך שננקט בקשר ל"המגן 1", על משרד הבריאות היה ללוות את תהליך הפיתוח באמצעות מומחים חיצוניים ובלתי תלויים לאבטחת מידע מראשיתו. שקיפות בדיעבד יכולה להשיג תוצאה דומה. נציין כי בנוגע ל"המגן 1" התברר שהקוד שפורסם היה חסר וחלקי לעומת הקוד שהופעל ביישומון, ולאחר פניה למשרד הבריאות, הפער תוקן.[1]
- יש למנות "ממונה הגנת פרטיות" (Chief privacy Officer) בקשר עם "המגן". גם כאן, השילוב בין הצוות הטכנולוגי לרשות להגנת הפרטיות הניב תוצאות משביעות רצון, אולם לאחר הפיתוח הראשוני, יש לוודא המשך של התהליך לאורך זמן.

<u>חשיבות השימוש ביישומון</u>

לאור הסקירה לעיל, פרטיות ישראל רואה חשיבות רבה בהפצה ושימוש נרחב של יישומון "המגן 2", בפרט לאור היתרונות הבולטים של "המגן 2" על חלופות קיימות אחרות באיתור מגעים (איכוני השב"כ, יישומונים מסחריים) כמפורט להלן -

1. **מערכת מבוזרת**: נתוני המגעים המיקומים נשמרים במכשיר הסלולרי של המשתמש, ולא בשרת מחשב מרכזי שנמצא בשליטה של רשויות המדינה או חברות פרטיות. השימוש בשרת מרכזי מאפשר להצליב את נתוני המיקום עם מידע אישי נוסף ובכך לבצע ניתוחי מידע נוספים שאינם ידועים למשתמש.
2. **דיוק באיתור מגעים**: עד היום, על מנת לאתר מגעים באמצעות כלים טכנולוגיים, נעשה שימוש בטכנולוגיה של אותות GPS או איכון סלולרי (המגן 1 וכלי המעקב של השב"כ). טכנולוגיה זו אינה

[1] ראו את דיווחו של רן בר-זיק "הקוד של אפליקציית המגן פתוח, אבל בתוכו הסתתרו הפתעות" הארץ 26.7.2020, נמצא ב: https://www.haaretz.co.il/captain/software/.premium-1.9018639.

מאפשרת לזהות מגע קרוב עם חולה, ואינה יעילה במקרים רבים (לדוגמה בתוך מבנים ובערים צפופות).

3. **פתרון וולונטרי**: הורדה ושימוש ב"המגן 2" הם וולונטריים (בניגוד למעקבי השב"כ). כמו גם, דיווח על מגעים והעברת מידע למשרד הבריאות תלויה בהסכמה מדעת של המשתמש. במידה והמשתמש בוחר לשתף עם משרד הבריאות נתוני מיקום, משרד הבריאות מציע לבצע הליך של מחיקה של מידע רגיש (כמו כתובת מגורים ומקום העבודה).
4. **שימוש בקוד פתוח**: משרד הבריאות פיתח את "המגן" באמצעות שימוש במתודולוגיית קוד פתוח. היתרון המרכזי בכך הוא שהקוד של היישומון פתוח לציבור וכל אדם רשאי לעיין בקוד, לבדוק אותו, להעיר ולהוסיף עליו.

על אף היתרונות הבולטים, יש ליישומון גם חסרונות: היעילות באיתור המגעים תלויה במידת התפוצה שלו. על מנת לזהות מגעים באמצעות בלוטות', היישומון צריך להיות מותקן על שני המכשירים (של החולה ושל מי שבא איתו במגע). הצורך באיסוף נתוני מיקום, בנוסף לנתוני מגעים (בלוטות'), אינו ברור דיו ואף יכול להוות בסיס לעיבוד מידע שעשוי לחשוף מידע רגיש על אודות המשתמש (לדוגמה, במצב שבו מצליבים בין נתוני המיקום לנתוני הבלוטות' ניתן להסיק על אודות קשרים חברתיים ואישיים: עם מי אדם נפגש, כמה זמן הוא היה במחיצתו והמקומות שבהם הם נפגשו).

תוך שקילת היתרונות אל מול החסרונות, פרטיות ישראל סבורה שהפצה ושימוש ביישומון "המגן 2" מאזן באופן הולם בין הזכות החוקתית לפרטיות לבין הצורך בניטור ואיתור חולים בצורה יעילה ואפקטיבית. זאת בניגוד, לפתרון הדואלי שקיים כיום – איכוני השב"כ המאפשרים למדינה לעקוב אחר חולים ואנשים שבאו במגע עם חולים באופן כפוי, ריכוזי ושאינו שקוף לציבור – ולצידם שימוש ביישומון אזרחי.

פרטיות ישראל סבורה שהפצה רחבה של "המגן 2" עשויה לסייע לקטוע את שרשראות ההדבקה ביעילות רבה מזו של מעקבי השב"כ, להגביר את אמון הציבור בפעולות הממשלה, לקדם ערכים של ערבות הדדית בעת מצוקה - ולעשות כל זאת אגב כיבוד הזכות החוקתית לפרטיות. פרטיות ישראל קוראת לקדם את השימוש ב"המגן 2" במהירות ובנחישות, לפתור במהירות את בעיות הטכנולוגיה והממשק שהתגלו עם שחרורו ולהקדיש להטמעתו בציבור תקציבי פירסום הולמים, באופן שיאפשר לחדול במהירות הרבה ביותר מהמעקב הפולשני של שירות הביטחון הכללי אחרי נתיבי התנועה וההדבקה של חולי קורונה והאנשים שעימם נפגשו.

תקציר ממצאי הסקירה הטכנולוגית - המגן 2

חטיבת הגנת הפרטיות וצוות התקיפה של מרכז הגנת הסייבר ב-BDO ישראל ערכו, לבקשת עמותת פרטיות ישראל, סקירה טכנית ליישומון המגן 2 שמטרתה לבדוק:

1. האם מתבצעת העברת מידע מהיישומון לצדדים שלישיים;
2. האם המידע שהיישומון אוסף נשמרים בצורה מאובטחת ומוצפנת;
3. אלו הרשאות היישומון מבקש וכיצד נעשה שימוש בהרשאות אלו (לדוגמה: גישה לאנשי קשר, גלריית תמונות וכיו"ב).

לאור המגבלות הברורות, הבדיקה לא כללה מצב בו היישומון מזהה מגע עם חולה מאומת. כמו כן, הבדיקה לא כללה סקירה של הקוד שפרסם משרד הבריאות באתר GitHub, אלא נערכה על היישומון שזמין בחנויות האפליקציות.

ממצאי הבדיקה הראו כי -

1. לא מתבצעת העברת מידע מחוץ למכשיר בתנאים שנבדקו.
2. המידע מוצפן ומאובטח. המידע שנשלח אל היישומון, וכן המידע שהיישומון מייצר נשמרים באופן מוצפן ומאובטח, כך שאין דרך אפקטיבית לגשת למידע שלא באמצעות האפליקציה. משמעות הדבר, שניצול חולשות ביישומים אחרים במכשיר לא יכול להוביל באופן מעשי לדלף מידע שמאוחסן ביישומון המגן 2.
3. אין שימוש חורג בהרשאות. היישומון מבקש הרשאות למספר רכיבים ויישומים במכשיר. מהבדיקה עולה כי אין גישה ליישומים במכשיר המכילים מידע אישי כמו אנשי קשר, גלריית תמונות וכיו"ב ואין ניצול עודף של הרשאות קיימות, שלא לצורך איתור מגעים.

עמותת פרטיות ישראל ופירמת BDO ימשיכו לפעול באופן יזום ולקדם תהליכים ובדיקות על מנת לוודא כי ארגונים, בפרט ממשלתיים, מתייחסים באופן נאות להיבטי פרטיות ואבטחת מידע.

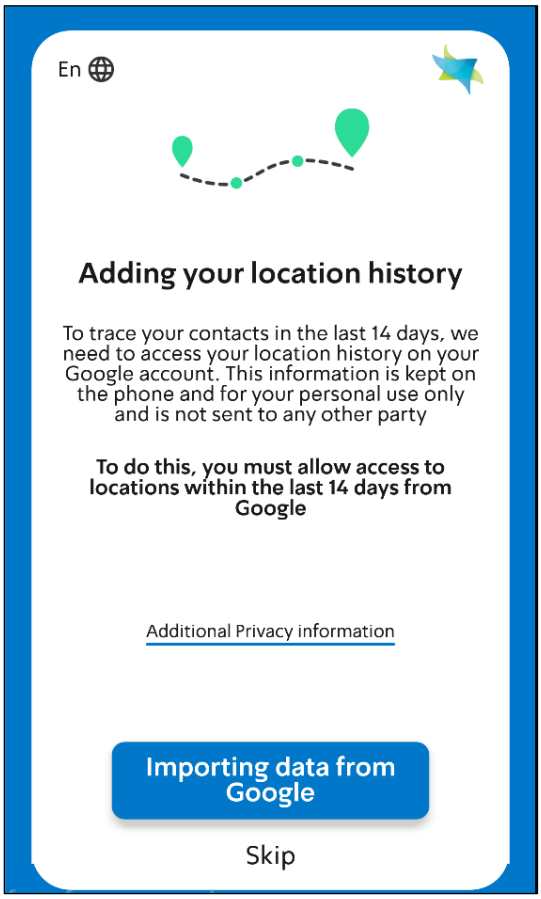
להלן חלק מן הממצאים של הדוח:

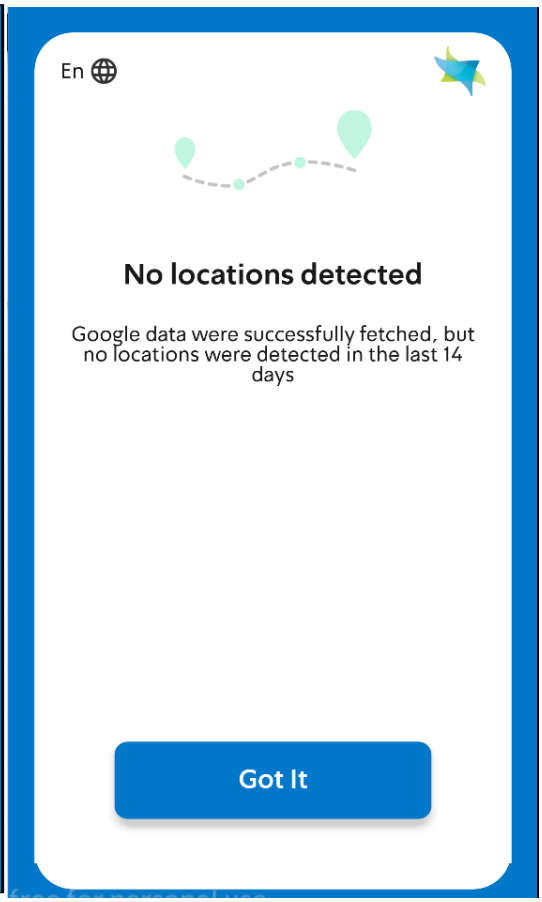
הדו"ח המלא כולל מס' מצומצם של ליקויי אבטחה שנמצאו באפליקציה. למיטב שיקול הדעת של BDO אלה אינם ליקויים מהותיים המסכנים את המשתמש. הליקויים הללו הועברו במישרין למשרד הבריאות לבחינה ולהמשך טיפול.

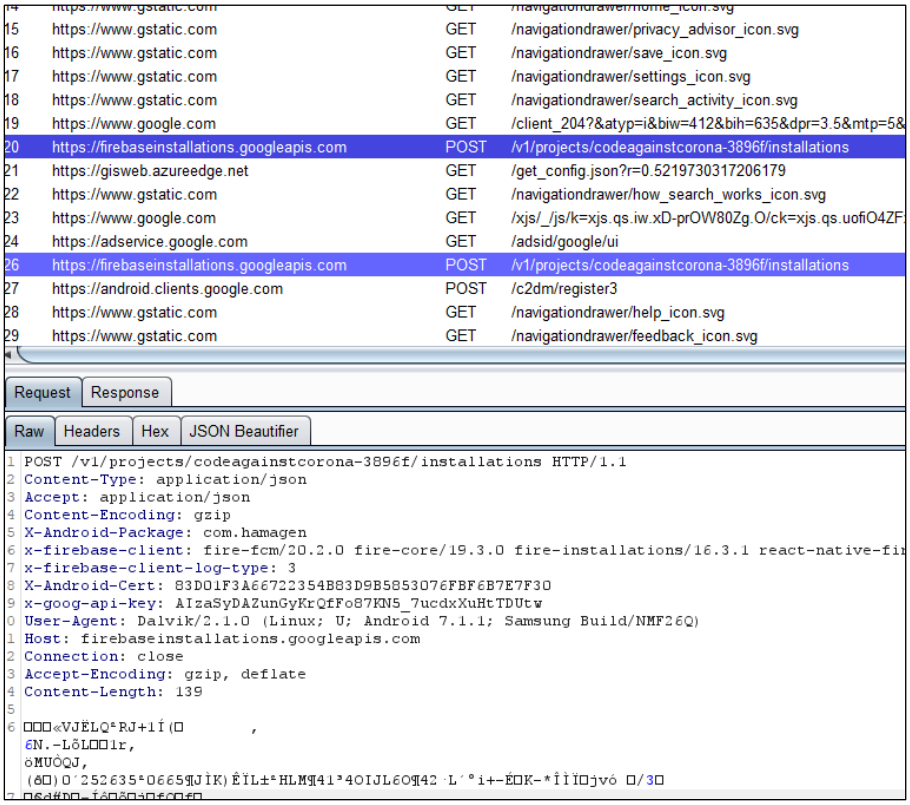
On August 2020 BDO conducted a mobile application analysis for Hamagen 2 version 2.2.6 (Android Version).

1.1 Installation and First Launch

During the first launch of the application, it prompts a user to allow an access to the Google account in order to retrieve location history from the past 14 days. This process is performed within a WebView frame inside the application by using google API and gstatic.com.

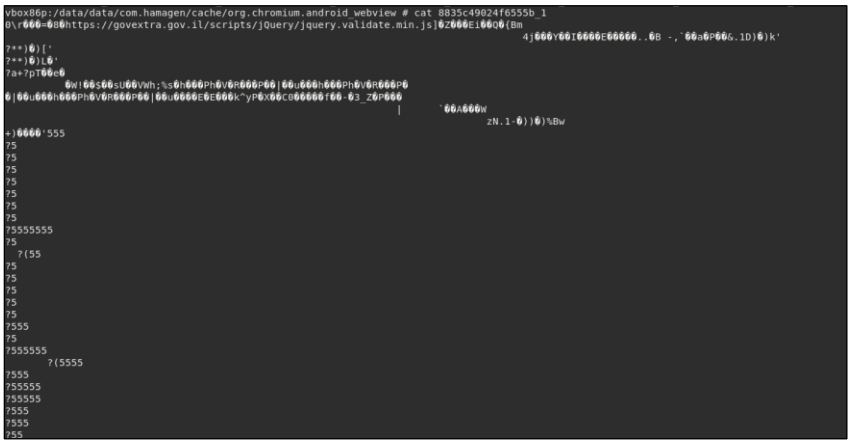






1.2 Data Storage

No data stored in clear text, all data stored on the device encrypted:



1.4 Permissions

The following screenshot represents permissions that the Magen App requires when installed. As it is possible to see the Magen App requires a lot of different permissions for proper functioning. Full description and explanation regarding all permissions presented at section 3.0.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-feature android:name="android.hardware.bluetooth_le" android:required="false"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <uses-permission android:name="android.permission.ACTIVITY_RECOGNITION"/>
    <uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"/>
    <uses-permission android:name="com.google.android.gms.permission.ACTIVITY_RECOGNITION"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="oppo.permission.OPPO_COMPONENT_SAFE"/>
    <uses-permission android:name="com.huawei.permission.external_app_settings.USE_COMPONENT"/>
    <uses-feature android:name="android.hardware.location.gps" android:required="false"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-feature android:name="android.hardware.bluetooth" android:required="false"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
    <uses-permission android:name="com.android.vending.CHECK_LICENSE"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
```

1.5 Conclusion

From the analysis, we haven't identified any form of the application sending user or device sensitive information to any remote party including MoH, therefore we can safely assume that it is indeed performing the cross reference check with confirmed patients, locally on the device.

BDO ISRAEL is a dynamic and business oriented accounting and consulting firm ranking amongst the five leading accounting firms in Israel. The firm was established in 1983, employs over 1,600 employees through 10 branches in Israel.
BDO's Cybersecurity Center was established over 16 years ago and is among the largest information security and cyber security consulting unit in Israel.
The Data Protection Division within the center is a leading body in Israel in implementation, management and control of privacy, cybersecurity, and business continuity management systems, laws, regulations and standards.