19 יוני 2022
כ' בסיוון תשפ"ב

הגנה על הפרטיות בעת שימוש בכלי תחבורה זעירים שיתופיים

רקע

תופעת השימוש בכלי תחבורה זעירים שיתופיים התגלתה בשנים האחרונות כבעלת יתרונות רבים במרחב העירוני, ובהם שיפור הניידות האישית, הפחתת זיהום אוויר, הפחתת גודש התנועה ועוד. תופעה זו, שיש גם הקוראים לה "ניידות זעירה" (Micro Mobility), מיוצגת על-ידי מגוון רחב יחסית של אמצעי תחבורה קומפקטיים וקלי משקל ובהם: קורקינטים חשמליים (גלגינוע), סקייטבורדים חשמליים (גלגשת), אופניים חשמליים, הוברבורד/סגווי (רכינוע) ועוד.

מבין אמצעי התחבורה הללו, קורקינטים חשמליים הם הנפוצים ביותר בקרב המשתמשים,[1] וזאת בשל היותם ניידים ופשוטים לתפעול, באופן המאפשר השתלבות בתנועה עירונית בקלות ובזריזות, ובשל יכולתם להגיע ליעדים קרובים יחסית שהתאימו בעבר להליכה. ההיבט הבולט ביותר של הקורקינטים החשמליים הוא הפוטנציאל שלהם לחבר בין נקודות הסיום של תנועת התחבורה הציבורית/תנועת הרכבים (כמו חניונים ותחנות אוטובוס), לבין יעדים סופיים כמו מקומות עבודה ומבני קמפוסים, באזורים צפופים או מקומות עם נגישות מוגבלת לכלי תחבורה גדולים (כמו מכוניות או אוטובוסים).[2] השימוש בקורקינטים החשמליים השיתופיים גם חוסך למשתמשים עלויות תחזוקה וביטוח הכרוכות בבעלות על רכב, ועלויות נסיעה או שיתוף נסיעה עבור נסיעות למרחקים קצרים, שהן יקרות יחסית. יתר על כן, התהליך הפשוט של זיהוי המיקום של הקורקינט החשמלי באמצעות אפליקציה של ספק השירות, אפשרויות תשלום נוחות למשתמשים ואפשרויות חניה גמישות, הופכים את שירותי הקורקינטים לאטרקטיביים במיוחד עבור נוסעים במרחב העירוני.

עם זאת, בשימוש בכלי תחבורה חשמליים שיתופיים גלומים אתגרי פרטיות משמעותיים, הנובעים בעיקרם מהעברת נתוני מיקום על אודות המשתמשים. העברת נתוני המיקום חיונית לצורך הפעלת השירות, ואולם מדובר במידע אישי בעל ערך כלכלי עבור גופים רבים, וקיים חשש לשימוש במידע האישי שלא למטרה לשמו נאסף ולהגברת פוטנציאל הפגיעה בפרטיות המשתמשים.

---

[1] שוק ההכנסות במגזר הקורקינטים החשמליים השיתופיים הגלובלי מוערך בכ-1.4 מיליארד דולר בשנת 2021. ההכנסות צפויות להציג קצב צמיחה שנתי של 15.32%, מה שיביא להיקף שוק חזוי של 2.8 מיליארד דולר עד שנת 2026. מספר המשתמשים בקורקינטים חשמליים שיתופיים צפוי להסתכם ב-125.4 מיליון משתמשים ברחבי העולם עד שנת 2026. 100% מסך ההכנסות יופקו באמצעות מכירות מקוונות עד שנת 2026.
https://www.statista.com/outlook/dmo/eservices/fitness/wearables/worldwide

[2] "פתרונות למייל האחרון" (Last Mile) – מושג זה מתייחס למגמת ההתפתחות של פתרונות תחבורה המספקים מענה תחבורתי לחלק הדרך שנמצא בין נקודות הסיום של התחבורה הציבורית או הרכבים, לבין היעד הסופי של המשתמש, בהם גם השימוש בכלי תחבורה זעירים, המאפשרים ניידות ללא תחנות או קו מוגדר, וזאת על פי רוב בהפעלה עצמית. על מגמות טכנולוגיות בתחבורה חכמה ועל ההתפתחויות המרכזיות בעולם התחבורה ראו 'מדריך הגנת הפרטיות בגופי תחבורה בסביבה דיגיטלית' (אוגוסט 2020) שפורסם על ידי הרשות להגנת הפרטיות:
https://www.gov.il/BlobFolder/news/guide-transportation-privacy/he/--transformation--privacy--2020--.pdf

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 תל אביב, 7360, ת.ד. קרית הממשלה

הרשות להגנת הפרטיות ניתחה את מסמכי מדיניות הפרטיות ותנאי השימוש של אפליקציות המשמשות את חברות הקורקינטים השיתופיים המרכזיות בישראל, וגיבשה סדרה של המלצות לשימוש בטוח ומאוזן תוך שמירת על פרטיות המשתמשים.

מסמך זה מתמקד בקורקינטים חשמליים שיתופיים ומטרתו היא להציב זרקור על התופעה, לסקור את דרישות הדין ולהציע המלצות להתנהלות נכונה לשם צמצום הפגיעה בפרטיות המשתמשים.

יובהר כי המסמך אינו מבקש למנוע את השימוש בקורקינטים חשמליים שיתופיים, אלא לתת כלים להתנהלות נכונה של המשתמשים בהיבטי פרטיות.

<u>נתוני מיקום – סקירה משפטית</u>

איסוף ועיבוד נתוני המיקום של אדם פוגעים באופן משמעותי בפרטיותו. לשם השוואה, רגולציית הגנת המידע האישי של האיחוד האירופי (GDPR) רואה בנתוני מיקום מידע פרטי הראוי להגנה. בישראל, נקבע בפסק הדין בעניין **חברות הסיעוד**,[3] כי "פעמים רבות, מיקומו של אדם עלול לחשוף פרטים שהם בליבת הזכות לפרטיות כגון המצב הבריאותי". בעניין **האגודה לזכויות האזרח**[4] קבע בית המשפט העליון כי נתוני מיקום הוכרו בחקיקה ובפסיקה ככאלה אשר קיימת לגביהם רגישות רבה, והם זוכים **להגנה מיוחדת בחקיקה**,[5] וניתן ללמוד מהם על קיומם של קשרים אישיים ומפגשים חברתיים. לאחרונה הוסיף וקבע בית המשפט העליון בעניין **פלונית**, אשר עסק בסוגיה של מתן צו שיפוטי לשם קבלת נתוני איכון טלפון סלולרי, כי "נתוני מיקום עשויים ללמד רבות על אורחות חייו ומאפייניו של מושאם, כך שחשיפתם לזולת עשויה אף להסב לו נזקים של ממש במגוון תחומים". עוד נקבע באותו עניין כי "הפגיעה הטמונה בגילוי נתוני מיקום ללא הסכמתו של מושא האיכון, באה לידי ביטוי, בעיקרו של דבר, בעצם חשיפת תנועותיו של הפרט והיותן מושא לתשומת לבו של אדם אחר. זאת, אף אם אין הפרט מבקש לחסות נתון ספציפי זה או אחר מתוך נתונים אלה".

מנתוני מיקום כשלעצמם, או בשילוב עם אינפורמציה ממקורות נוספים, ניתן אפוא להסיק מידע רגיש ביותר על אישיותו של אדם, צנעת אישותו, מצבו הכלכלי ועוד פרטי מידע המוגנים לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות").[6] כך לדוגמה, הימצאותו של אדם במרפאה, עלולה להעיד על מצב בריאותו, הגם שביקש שלא לשתף בכך אף אדם; הימצאותו של אדם בבית תפילה של עדה מסוימת עשויה להעיד על אמונתו הדתית; וכיוצא באלה.

---

[3] עת"מ 28857-06-17 **עמותת חברות הסיעוד נ' משרד הביטחון** (פורסם בנבו, 01.07.2019), פסקה 16.4 (להלן: "עניין עמותת חברות הסיעוד"). על פסק הדין הוגש ערעור מטעם המדינה לבית המשפט העליון, אולם המדינה לא השיגה על קביעות בית המשפט המחוזי בהיבטי הפרטיות, ואלו נותרו על כנן גם לאחר פסק הדין בערעור (ראו עע"מ 6466/19 **משרד הביטחון נ' עמותת חברות הסיעוד** (פורסם בנבו, 11.10.2020), פסקה 8 לפסק הדין).

[4] בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת** (פורסם בנבו, 01.03.2021), פסקה 18 לפסק-דינה של הנשיאה חיות. ראו גם פסקה 5 לפסק-דינה של השופטת ברון.

[5] ראו פרט 1(3)(ו) בתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, המפנה להגדרת "נתוני תקשורת" בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח-2007, שכוללת בין היתר נתוני מיקום. ראו גם בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל נ' משטרת ישראל** (פורסם בנבו, 28.5.2012), פסקה 7 לפסק-דינה של הנשיאה בייניש.

[6] להרחבה על סוגי הנתונים המוגנים לפי חוק הגנת הפרטיות, ראו טיוטת גילוי הדעת של הרשות להגנת הפרטיות "מהם "מידע" ו"ידיעה על עניינו הפרטיים של אדם" בחוק הגנת הפרטיות". <u>גילוי הדעת פורסם להערות הציבור והוא זמין באתר הרשות</u>.

איסוף נתונים אישיים למטרות נסיעה שיתופית

קורקינטים חשמליים שיתופיים מתבססים, בין היתר, על איסוף נתונים על אודות המשתמש ובעיקר על מיקום המשתמש, לשם הפעלתם בצורה מיטבית. כך, בין היתר, נאספים על-ידי אפליקציות לשימוש בקורקינטים חשמליים שיתופיים הנתונים הבאים:

- **נתוני מיקום** ו/או תיעוד של נסיעות בודדות והיסטוריית נסיעות, הכולל גם תיעוד של זמני נסיעה, הנאספים באמצעות GPS (מערכת מיקום גלובלית);
- **נתוני טלמטריית מיקום** – כל נתון שמתעד את התנועות ואת קריאות החיישנים מהכלי השיתופי הכולל מיקום, כיוון, מהירות, תנוחת בלם/מצערת וכו';
- **נתונים מפרטי חשבון המשתמש ונתונים נוספים המוזנים לאפליקציה** – ובהם שם, כתובת דוא"ל, מספר טלפון, תאריך לידה, מגדר, פרטי כתובת מגורים או מקום העבודה, פרטי אמצעי התשלום, היסטוריית דיווחי המשתמש, וכן כלל האינטראקציות המבוצעות על-ידי האפליקציה ובהן אינטראקציות למול ספק השירות השיתופי וכן אינטראקציות עם צדדים שלישיים במהלכן משותפים נתוני המשתמש לצרכי פרסום ושיווק;[7]
- **מידע ביומטרי** – תמונות של רישיון הנהיגה או תעודת הזהות של המשתמש, אשר בשל איכות הצילום כיום, הן למעשה מקור להפקת נתונים ביומטריים על אודות המשתמש.

נתונים אלו מועברים באופן מקוון ליישום סלולרי או למאגר מידע אחר, כך שניתן לנתח אותם בהמשך לאורך זמן.

נתונים אלו נאספים גם על ידי גופים שלטוניים. כך לדוגמה, מתקיימת העברת מידע בין ספקיות השירות לרשויות מקומיות.[8] יחד עם הצמיחה המהירה של שימוש בקורקינטים חשמליים משותפים, רשויות מקומיות ברחבי ישראל מקדמות מיזמי קורקינטים חשמליים שיתופיים בשטחן, תוך שהן דורשות גישה לנתונים הנאספים על ידי ספקיות השירות באמצעות רגולציה וחוזה ההפעלה, בין היתר כדי לקדם יעדים ציבוריים כגון שיפור הבטיחות, שוויון בנגישות לתחבורה וקיימות.

יצוין, כי במסגרת פיקוח רוחב שערכה הרשות להגנת הפרטיות ב-70 רשויות מקומיות בישראל נמצא כי פוטנציאל הסיכון לפרטיות ברשויות המקומיות, גם בהשוואה למגזרים שונים במשק, גבוה במיוחד.[9]

---

[7] אשר למסירת פרטיו האישיים ופרטי ההתקשרות של משתמש בקורקינט חשמלי על-ידי החברה המשכירה לצד שלישי הטוען שנפגע מרכיבתו, ראו פסק-דינו של בית משפט השלום בתל-אביב מן העת האחרונה בת"א 61142-07-21 **יעקב (קובי) כהן נ' ווינד תל-אביב (בייקי) בע"מ** (פורסם בנבו, 2.4.22). נכון לעת הזו טרם נקבעה הלכה מחייבת בנושא, וכעולה מפסק-הדין דומה כי הדין בסוגיה זו מצוי בשלביו הראשונים וצפוי להתפתח ולהתגבש במהלך השנים הקרובות.

[8] המידע הנאסף על ידי רשויות מקומיות כולל את פילוח המשתמשים ברמה חודשית לפי קבוצת גיל, מגדר, עיר וארץ מגורים, תדירות שימוש וכן כל מידע נוסף אודות המשתמש. ראו למשל סעיף 5 להזמנה של עיריית ראשון לציון להפעלת שירותי השכרת קורקינטים חשמליים שיתופיים; סעיף 7 לקול הקורא של עיריית תל אביב להגשת בקשות למתן היתר זמני להצבת כלים זעירים שיתופיים להשכרה במרחב הציבורי לשנת 2022; סעיף 6 לקול קורא מספר 2021/21 של עיריית חולון לקבלת היתר להפעלת מערך קורקינטים חשמליים; סעיף 7 להרשאה להפעלת מערך קורקינט חשמלי ביהוד מונוסון.

[9] הרשות להגנת הפרטיות פרסמה דו"ח ממצאי פיקוח רוחב בקרב רשויות מקומיות ביום 22.11.21

הסיכונים לפרטיות

כאמור, השימוש הנפוץ בקורקינטים חשמליים שיתופיים נובע מיעילותם וזמינותם. עם זאת, קיים חשש שמידע אישי, הכולל גם נתונים פיננסים כדוגמת כרטיסי האשראי של המשתמש, ונתוני מיקום הנשמרים במאגרי המידע של החברות המפעילות את הקורקינט השיתופי, יזלגו לידי צדדים שלישיים, או שייעשה בהם שימוש שחורג מן המטרות אשר לשמן נאסף המידע האמור. מכאן הסיכון לפרטיות המשתמשים. להלן, נבקש להציג מספר נקודות מרכזיות שבהן הפוטנציאל לפגיעה בפרטיות המשתמשים גדול:

מידע אישי באפליקציה השיתופית

כמפורט לעיל, שימוש באפליקציה המספקת שירותי קורקינטים חשמליים שיתופיים כרוך באיסוף ובעיבוד מידע אישי רב ורגיש על אודות משתמשים, המייצר, בין היתר, "שובל דיגיטלי" של נתוני מיקום, אשר מגילויים עלול להיחשף מידע רגיש על חייו והרגליו של אדם. עובדה זו מגבירה את סיכוני אבטחת המידע, ומעלה את החשש כי המידע שייאסף במסגרת השימוש באפליקציה, יזלוג לגורמים שאינם מורשים על ידי התחזות, חדירה מרחוק או תקיפה.

מידע אישי במעבר

כאשר נתונים נמצאים במעבר, הם עשויים להיות חשופים להאזנות, כמו Sniffing (תהליך ניטור ולכידת כל החבילות העוברות ברשת נתונה) או Tapping (התקן חומרה המשמש לגישה לנתונים הזורמים ברשת מחשבים), וכן לשינוי או ניתוח התעבורה. דוגמא נוספת היא האזנת סתר – יירוט בזמן אמת של תקשורת פרטית. התקפות אלו מהוות איום משמעותי, שכן הן יכולות לחשוף את המידע האישי של המשתמש בפני התוקף.[10]

קורקינטים חשמליים משותפים, מצוידים באופן אוניברסלי בבקר מובנה הניתן להפעלה באמצעות אפליקציה התואמת להם. הקורקינטים מתקשרים עם האפליקציה באמצעות Bluetooth Low Energy (BLE)[11] או באמצעות רשת האינטרנט. קורקינטים חשמליים מסתמכים בעיקר על BLE שמשדרת חבילות (פאקטים) במרווחים קבועים שאותם ניתן ללכוד על ידי סמארטפונים. חבילות אלו מכילות מזהים ייחודיים המסייעים בזיהוי הקורקינטים החשמליים ממכשירי BLE אחרים. כדי להפעיל או להפסיק את השימוש ברוב הקורקינטים החשמליים, ה-BLE ונתוני האינטרנט צריכים להיות פעילים וזמינים.

שימוש בערוצי תקשורת כאלה פותח אפשרות לפוטנציאל גדול של התקפות, שחלקן יכולות להיות יעילות במיוחד לגבי קורקינטים חשמליים שיתופיים והחברות המפעילות את השירות. באופן דומה, השימוש בענן לניהול ההשכרה ונתוני המשתמשים יכול להפוך למטרה.

---

[10] IoT Penetration Testing: Hacking an Electric Scooter: https://kth.diva-portal.org/smash/get/diva2:1334205/FULLTEXT01.pdf

[11] Bluetooth Low Energy היא שיטת תקשורת המיועדת לפעולה בצריכת חשמל נמוכה מאוד. בשיטת תקשורת זו מתאפשרת למפתחים גמישות לבניית מגוון גדול של מוצרים העונים על דרישות הקישוריות הייחודיות של השוק שלהם https://www.bluetooth.com/learn-about-bluetooth/tech-overview/.

מידע אישי באחסון אצל ספק השירות

על מנת לייעל את התחבורה והתכנון העירוני, חברות, חוקרים וגופים אחרים, נדרשים לאסוף, לאחסן ולעבד נתונים אנונימיים המכילים "חותמות מיקום" (קואורדינטות גיאוגרפיות וחותמות זמן) של משתמשים. מיזוג מערכי נתונים אלה, יכול לספק מידע עשיר על האופן שבו בני אדם נעים בסוגי התחבורה השונים. עם זאת, ניתוח חותמות מיקום יכול להגיע עד לרמת מידע על אדם קונקרטי כך שניתן לעשות בהן שימוש למטרות מסחריות ואחרות. כך לדוגמה, מחקר של MIT[12] מגלה שהפרקטיקה ההולכת וגוברת של הידור[13] (Compiling) מערכי נתונים מסיביים ואנונימיים על דפוסי תנועה של אנשים, יכולה לספק תובנות עמוקות לגבי התנהגות אנושית לצרכי מחקר, אך היא גם עלולה לחשוף את הנתונים האישיים של נושאי המידע לסיכונים שונים.

מחקרים נוספים[14] הראו שבהינתן רק כמה נקודות שנבחרו באקראי במערך נתונים של ניידות, ניתן לזהות וללמוד מידע רגיש על אנשים. ובהקשר שלנו: ניתן להצליב נתוני מסלולי נסיעה של משתמשים אנונימיים ממאגר נתונים אחד, עם נתוני משתמשים שעברו תהליך דה-אנונימיזציה לנתונים מזוהים ממאגר נתונים אחר, כדי לחשוף את נושאי המידע של הנתונים האנונימיים.

גישה של צד שלישי לנתונים המופקים על ידי ספקיות השירות

לנוכח רגישותו של המידע הנאסף וערכו הכלכלי, קיים חשש כי גורמים בעלי אינטרסים יבקשו לעשות שימוש במידע למטרות מסחריות, שאינן חלק מהמטרות לשמן נאסף המידע (הקשורות בליבתן להיבטים השונים של תפעול השירות). שימוש שכזה במידע ללא הסכמת המשתמש מהווה, מטבע הדברים, פגיעה חמורה בפרטיות. סיכון זה מתחדד שעה שמפעילי האפליקציות של הקורקינטים השיתופיים, האמונים על איסוף המידע ושמירתו, הם גורמים פרטיים בעלי אינטרסים כלכליים, ויכול להיווצר עבורם תמריץ לעשות שימוש במידע גם לשם הפקת רווחים.

---

[12] D. Kondor, B. Hashemian, Y. -A. de Montjoye and C. Ratti, "Towards Matching User Mobility Traces in Large-Scale Datasets," in IEEE Transactions on Big Data, vol. 6, no. 4, pp. 714-726, 1 Dec. 2020, doi: 10.1109/TBDATA.2018.2871693.

[13] הידור הוא מונח מחשובי המבטא תרגום משפת מחשב אחת לשפת מחשב אחרת. המהדר הקלאסי מקבל כקלט תכנית הכתובה בשפה עילית ומתרגם אותה לתוכנית בשפת מכונה.

[14] de Montjoye, YA., Hidalgo, C., Verleysen, M. *et al.* Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep* **3**, 1376 (2013). https://doi.org/10.1038/srep01376

המלצות להנהלות הציבור בעת שימוש בקורקינטים חשמליים שיתופיים

להלן יוצגו המלצות הרשות להגנת הפרטיות בנושא שימוש בקורקינטים חשמליים שיתופיים. ההמלצות מבוססות, בין היתר, על העקרונות והכללים שהוצגו קודם לכן:

בדיקת הגדרות הפרטיות באפליקציית ספק הקורקינט השיתופי

מומלץ לבדוק את מדיניות הפרטיות של האפליקציה בה אתם משמשים. בכל אפליקציה להפעלת כלי תחבורה זעיר שיתופי, נדרש ספק השירות לפרט מהם השימושים שתוכל החברה המפעילה לעשות בנתונים הנאספים על-ידה.[15] חפשו הגדרות אלו ובחנו, לפני מתן ההסכמה והרישום לאפליקציה, האם השימוש שצפויה החברה לעשות במידע האישי על נתוני המיקום והרגלי התחבורה שלכם, מקובל מבחינתכם. **ככל שלא מקובל עליכם – אל תאשרו את האפליקציה**.

לפני ההרשמה לאפליקציית ספק הקורקינט השיתופי

מומלץ להימנע מלקשר, לשתף, או להתחבר אל אפליקציית השירות באמצעות שירותי צד שלישי. מרבית האפליקציות של ספקי השירות מאפשרות למשתמש להירשם או להיכנס על ידי שירותים של צד שלישי (לדוגמא: חיבור על ידי חשבון פייסבוק או גוגל). דרך הרשמה זו מאפשרת לספק הקורקינט השיתופי לאסוף מידע עליכם מתוך חשבונותיכם ברשתות חברתיות או החשבון בגוגל, ועשויה לאפשר גם לענקיות המידע (פייסבוק, גוגל) לקבל מידע אישי מסוים מספק הקורקינט. זאת, למרות שמדובר במידע שלא התכוונתם לשתף. **הרשמה לשירות שלא דרך חשבון ברשת חברתית או חשבון מייל – מגנה יותר על פרטיותכם.**

הסכמה לשיתוף המיקום באפליקציית ספק הקורקינט השיתופי

אפליקציות הקורקינט השיתופי מבקשות להשתמש במיקום שלכם על מנת לספק שירותים טובים יותר. ברוב המכשירים הסלולריים ניתן לבחור לגבי כל אפליקציה באופן ספציפי, אם לתת לה גישה למיקום שלכם. שימו לב: יש אפשרות לתת גישה למיקום באופן רציף, לתת גישה למיקום רק בעת השימוש באפליקציה או לא לאפשר כלל לאפליקציה גישה למידע זה. **המלצתנו היא, ככלל, לא לתת לאפליקציה גישה למיקומכם.**

במהלך השימוש באפליקציית ספק הקורקינט השיתופי

הקפידו להטמיע עדכוני אבטחה שמפרסם מפעיל האפליקציה כדי להבטיח שהאפליקציה תהיה מוגנת מפני סיכוני אבטחה חדשים. עקבו אחר הרשאות הגישה של האפליקציה, גם בעת הורדת עדכוני תוכנה. **אם הורחבו ההרשאות באופן שמנוגד לרצונכם או מבלי שהובהר הצורך בהרחבה זו - שקלו למחוק את חשבון המשתמש ואת האפליקציה.**

[15] חוק הגנת הפרטיות מתייחס גם לזכויות נושא המידע. כך, על פי סעיף 11 לחוק, יש להודיע לנושא המידע על הכוונה לאיסוף המידע תוך פירוט מטרות השימוש במידע ותוך ציון האם יש חובה חוקית למסירת המידע או שמא הדבר נתון להסכמתו.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 תל אביב, 7360, ת.ד. קרית הממשלה

<u>סיום השימוש באפליקציית ספק הקורקינט השיתופי</u>

אם אתם משתמשים מזדמנים ונראה כי לא תדרשו יותר לשירות, או שהחלטתם להפסיק להשתמש בשירות הקורקינט השיתופי, מחקו את החשבון ואת האפליקציה של ספק השירות. כך תבטיחו כי האפליקציה תפסיק לאסוף מידע על מיקומכם ולשדרו, או לקיים אינטראקציה עם יישומים אחרים במכשיר. באפליקציות רבות המידע שלכם נשמר גם לאחר מחיקת החשבון. על כן, ממליצה הרשות לפנות לאתר ספק שירותי הקורקינט **ולוודא שהמידע האישי עליכם אכן נמחק בד בבד עם מחיקת החשבון.**