משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة القانون التكنولوجيا والمعلومات

מדריך הגנת הפרטיות בגופי תחבורה בסביבה דיגיטלית

אוגוסט 2020

Intelligent Transportation Systems (ITS) therefore pose sharp challenges to regulatory regimes that are concerned to protect privacy, but they also provide possibilities for designing privacy protection into the technologies themselves.

Colin Bennett, Charles Raab & Priscilla Regan, People and place: Patterns of individual identification within intelligent transportation systems (SURVEILLANCE AS SOCIAL SORTING PRIVACY, RISK, AND DIGITAL DISCRIMINATION, David Lyon, 2003)

מערכות תחבורה חכמות (ITS) מציבות אתגרים רגולטורים מורכבים הנוגעים לשמירה על פרטיות, אך הן גם מספקות הזדמנויות לעיצוב הגנת הפרטיות בשלב פיתוח הטכנולוגיות עצמן.

מדריך זה מוגש כמידע כללי לשירות הציבור וגופי התחבורה. הדין המחייב הוא חוק הגנת הפרטיות, התשמ"א-1981, התקנות שהותקנו מכוחו והנחיות הרשות להגנת הפרטיות.

הדוגמאות במדריך זה הובאו כהמחשה כללית בלבד ומציגות אפשרויות ליישום התוכן המובא במדריך. הדוגמאות אינן מתאימות כפי שהן לכל מקרה, ויש לבחון כל מקרה לגופו וליישם את הוראות החוק בהתאם.

בכל מקום בו מופיעה פנייה בלשון זכר או נקבה, הכוונה היא לפנייה לכלל המגדרים.

גופי תחבורה – שם כולל לגורמים העוסקים בהיבטים שונים של תחבורה, לרבות: גורמים המספקים תשתיות לתחבורה; גורמים המספקים שירותי תחבורה ציבורית; גורמים המספקים שירותים נלווים לתחבורה, חברות הזנק (סטרטאפ) בתחום התחבורה החכמה; וכן גורמים המפעילים כלי תחבורה במרחב העירוני.

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة القانون التكنولوجيا والمعلومات

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

מדריך הגנת הפרטיות בגופי תחבורה בסביבה דיגיטלית

אוגוסט 2020

WWW.PPA.JUSTICE.GOV.IL | PPA@justice.gov.il | 073-3928555
חפשו אותנו גם בפייסבוק | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

תוכן עניינים

הקדמה 5
פרק 1 | תחבורה חכמה 7
סביבת התחבורה בישראל 8
מגמות טכנולוגיות רלוונטיות 10
התפתחויות מרכזיות בעולם התחבורה 10
פרק 2 | פרטיות 13
הזכות לפרטיות על קצה המזלג 13
הרשות להגנת הפרטיות 13
פרק 3 | אתגרי הפרטיות בתחבורה חכמה 15
פרק 4 | החובות הכלליות בחוק ביחס לאיסוף ולשימוש במידע אישי 18
ניהול מאגרי מידע 18
תקנות הגנת הפרטיות (אבטחת מידע) 20
פרק 5 | עקרונות להטמעת טכנולוגיות חדשות 23
פרק 6 | נושאים במיקוד 27
שאלות מנחות לבדיקה עצמית 27
כלים לשימוש נכון בנתוני עתק (Big Data) 30
כלים לשימוש נכון במצלמות 32
תחבורה במרחב העירוני 35
יישומונים (אפליקציות) לתשלום ולתיקוף בשירותי תחבורה ציבורית 40
מידע אישי ברכב הפרטי שלך – מבט לעתיד 50

הקדמה

מערכת התחבורה בישראל ובעולם כולו מתפתחת בקצב הולך וגובר. במערכת זו פעילים גופים ציבוריים, גופים פרטיים, חברות הזנק (סטרטאפים) חדשניות, חברות רכב גלובליות מובילות בתחומן, ועשרות ארגונים שונים מהמגזר השלישי אשר שמו לעצמם מטרה לקדם את התחום ולהתאימו לצרכי המשתמשים בעידן הנוכחי.

בהחלטה מס' 2316 משנת 2017 התחייבה ממשלת ישראל לפתח את התחום ולהפוך את ישראל למובילה בעולם (להלן: "החלטת הממשלה" או "החלטת ממשלה 'תחבורה חכמה'" לפי העניין). החלטת הממשלה עוסקת בשני היבטים: האחד – קידום ותמיכה בחברות העוסקות בתחום (פיתוח התעשייה הישראלית), והשני – קידום פתרונות לסוגיות תחבורתיות בישראל. משרד התחבורה הוא הגורם המרכזי בפעילות הממשלתית הנעשית בתחום זה. המשרד פועל בשני מרחבים: האחד – מרחב של פתרונות תחבורתיים המצויים תחת אחריותו הישירה, והשני – מרחב פעילות של התעשייה והשוק הפרטי (אקו-סיסטם). בין מרחבים אלו ישנה לעיתים חפיפה.

בדומה לנעשה בישראל, ממשלות רבות בעולם מציבות את תחום התחבורה החכמה במיקום גבוה בסדר העדיפויות שלהן, ופועלות לגיבוש אסטרטגיה ודרכי פעולה מתאימות לקידומו. נראה כי אחת המגמות הבולטות היא השינוי בתפיסת תפקידו של הרגולטור כחלק ממהפכת התחבורה החכמה. במסגרת שינוי זה תפקידו של הרגולטור כמנהל וכמפעיל (Operator) של תחבורה – קטן, בעוד תפקידו כרגולטור מאפשר (Enabler) שמהווה פלטפורמה המסייעת בהספקת שירותי ניידות מיטביים על ידי השוק הפרטי – הופך משמעותי יותר. דוגמה הממחישה שינוי שורשי זה היא בנושא מאגרי מידע (ופרטיות המשתמשים). ככלל, משרדי התחבורה בעולם (ובישראל) נוטים להימנע מלהקים ולהפעיל מאגרי מידע הנמצאים בבעלותם, אלא יוזמים, מעודדים ומכווינים הקמה של מאגרים שכאלה על ידי שחקנים שונים, אחרים ופרטיים, שפועלים בשוק. אחת ההשפעות הבולטות של שינוי זה **היא התגברות פוטנציאל הסכנה לפרטיות משתמשים.**

כנגזרת מחזון הממשלה בתחום התחבורה החכמה ולמגמות החדשנות בעולם התחבורה, משרד התחבורה פועל ליצירת פתרונות ניידות אופטימליים לכלל תושבי המדינה ולמשתמשים בשירותי תחבורה. תפיסת המשרד היא כי שילוב הכוחות בין תשתית ואמצעי תחבורה לבין טכנולוגיה, יתרום למקסום האפקטיביות של מערכת התחבורה בישראל. לב ליבה של תפיסה זו היא התבססות על איסוף ושיתוף מידע (Data) כבסיס לתכנון, לפיתוח, ולפיקוח על השוק, ושימוש במידע הנאסף לשם קידום מהפכת "הניידות כשירות" בישראל (Maas – Mobility as a Service).[1]

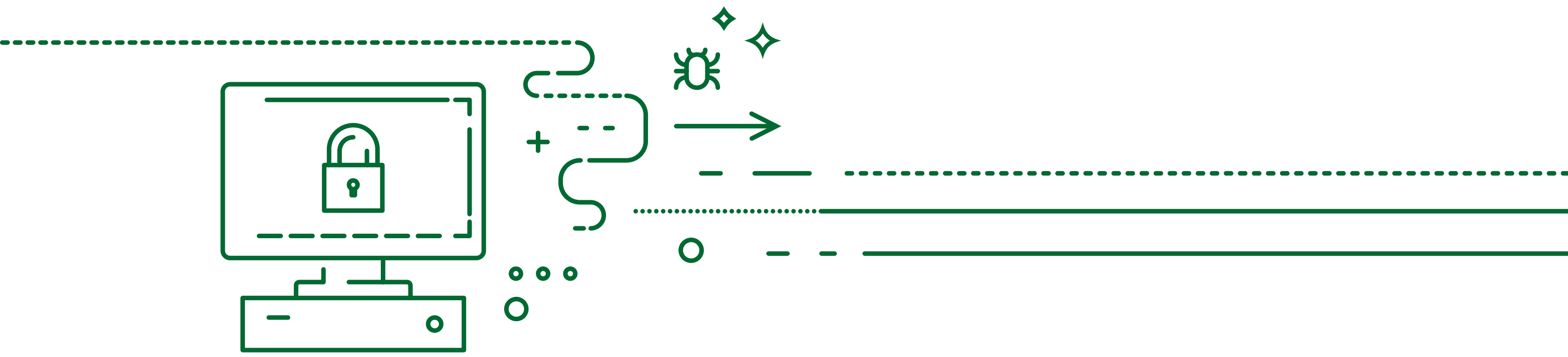
1 מתוך 'תחבורה חכמה', פעילות ותחומי מיקוד של משרד התחבורה והבטיחות בדרכים בתחום התחבורה החכמה, משרד התחבורה והבטיחות בדרכים, ספטמבר 2019

המידע הרב הנאסף מאפשר לממשלה ולרשויות העוסקות בתכנון תחבורה, להתאים תשתיות תחבורתיות למציאות המתפתחת ולשלוט בזרימת התנועה באופן יעיל יותר ובזמן אמת. מידע כזה כולל מידע עתק (Big Data), לרבות מיקום, זמני נסיעה, הרגלי שימוש בשירותי תחבורה ועוד. בנוסף, הנגשת המידע לציבור מהווה כלי למפתחי יישומים תחבורתיים. כלומר, מהפכת התחבורה החכמה מגבירה את הצורך בשיתופי פעולה וגישה הדדית למאגרי המידע הקיימים בין המפעילים הציבוריים והפרטיים. מצב זה מציב אתגרים טכנולוגיים רבים (כמו אבטחת מידע נאותה), אתגרים מסחריים (כמו זכויות בעלות על הנתונים) **ואתגרים אתיים ומשפטיים משמעותיים הנוגעים לפרטיות המשתמשים בתחבורה.**

במטרה להגן על פרטיות המשתמשים בשירותי תחבורה שונים, יש להכיר מספר עקרונות בסיסיים, וכן ליישם את עקרונות חוק הגנת הפרטיות, התשמ"א-1981 (להלן – 'חוק הגנת הפרטיות' או 'החוק') והתקנות הנלוות לו. **תפקידו של מדריך זה הוא להגדיר את הסיכונים לפרטיות בתחבורה בעידן הדיגיטלי ולספק לגופים ולחברות העוסקות בכך כלים נגישים להתמודדות עם סיכונים אלו.** מדריך זה מרכז בתוכו דפי מידע, שיטות עבודה מומלצות ועוד.

מדריך זה בנוי באופן מדורג כך שיאפשר הבנה כללית באשר לתחום התחבורה, מהי פרטיות ומהם אתגרי הפרטיות בתחום. המדרגה הראשונה כוללת הסבר מעמיק על הוראות חוק הגנת הפרטיות בדגש על איסוף ושימוש במידע אישי. השלב הבא הוא המדרגה הטכנולוגית אשר בה מפורטים העקרונות בתכנון והפעלה של שירותים בתחום התחבורה, בדגש על עיצוב לפרטיות (Privacy by Design). במדרגה האחרונה, מרוכזים דפי מידע בנושאים ממוקדים אשר נבחרו לאחר הבנת צרכי השחקנים בתחום.

הרשות להגנת הפרטיות מקווה כי מדריך זה יממש את מטרתו – **לסייע ולהבהיר את הדרך לאיזון נכון בין איסוף, עיבוד ושימוש במידע בעידן התחבורה החכמה לבין הצורך בשמירה על פרטיות המשתמשים בה.** נדגיש כי בהיות תחום התחבורה החכמה תחום חדש ודינמי החווה שינויים והתפתחויות תכופים יחסית, הרשות להגנת הפרטיות תעדכן מסמך זה מעת לעת.



פרק 1 | תחבורה חכמה

בשנים 'תחבורה חכמה' הוא מושג המבטא יישום אינטגרטיבי של מערכות טכנולוגיות למידע, תקשורת וניהול במערכות תחבורה, לרבות תשתיות תחבורה, כלי תחבורה והמשתמשים בהם. תחום רחב זה כולל מגוון אמצעים טכנולוגיים המאפשרים שינוי באופן ההתניידות של המשתמש: החל מאפליקציות לקידום נסיעות משותפות, דרך כלי תחבורה חדשים (כמו רכבים אוטונומיים וקורקינטים חשמליים) ועד הטמעת טכנולוגיות לניטור וניהול תנועה (המתבססות בין השאר על מצלמות ואמצעי ניטור) והטמעת תשתיות תקשורת מתקדמות לניהול תנועה. תחבורה חכמה נושאת עמה שינוי של ממש בעולם התחבורה. מהישענות על רכב פרטי לבחירה בין חלופות התניידות בהתאם לצרכי הפרט בכל נסיעה.

בכדי להנגיש למשתמשים היצע של חלופות, תחבורה חכמה יוצרת ומתבססת על מסד נתוני עתק (Big Data) כגון נתונים על מוצא, יעד, הרגלי נסיעה, המועברים לגופי התחבורה השונים ולרשויות, במטרה לשפר את שירותיהם. תחבורה חכמה עושה שימוש נרחב בחיישנים רבים כגון מצלמות, במידע המתקבל מהציבור ובאמצעים נוספים המספקים מידע שעל בסיסו ניתן לזהות את המשתמשים וצרכיהם בכל רגע נתון, וזאת לצרכי מערכות ניהול ובקרת תנועה מבוססות נתונים (Data Driven Traffic Management).

בבואנו לבחון מה עיקר משמעותה של תחבורה חכמה במדינת ישראל, נמצא כי היא כוללת שני תחומי ליבה:

1. **איסוף ושיתוף מידע (כולל נתוני עתק) כבסיס לתכנון, פיקוח ולפיתוח השוק –** פעולות אלו מהוות כלי מפתח לייעול והגברת האפקטיביות של שירותי התחבורה. תחום זה כולל גם את הנגשת המידע למפתחי יישומים תחבורתיים ולגופי תחבורה. יודגש כי תחום זה הופך את גופי התחבורה הפרטיים לבעלי מאגרי מידע על המשתמשים.
2. **פלטפורמת ניידות כשירות (MaaS – Mobility as a Service) –** תחום זה מאפשר שילוב בין אמצעי תחבורה שונים – ציבוריים, שיתופיים ואף פרטיים – והנגשתם למשתמשים דרך פלטפורמות אחודות, בהן ניתן לתכנן מסלול על פי עדיפות שמגדיר המשתמש. יודגש כי תחום זה משמעותו שילוב של מידע על משתמשים בין מספר גופי תחבורה וניתוחו.

בשני תחומי ליבה אלו יש פוטנציאל גבוה לפגיעה בפרטיות המשתמשים ב'תחבורה חכמה'.

סביבת התחבורה בישראל

כפי שצוין, תחום התחבורה מתפתח בקצב גובר ומכיל שחקנים רבים ושונים. את התחום ניתן לחלק במספר אופנים: בחלוקה טכנולוגית, חלוקה לפי שירותים ועוד. לאחר סקירה ומפגשים עם שחקנים מובילים בתחום, נבחרה החלוקה שלהלן על מנת להציב בתבנית את השחקנים הרלוונטיים לתחום, ובעיקר בכדי לייצר מענה מותאם לצרכים השונים של הקבוצות השונות.

מגזר ציבורי

השחקנים הרלוונטיים לתחום התחבורה במגזר הציבורי כוללים גופים ממשלתיים ורגולטוריים, כמו משרד התחבורה, משרד המשפטים והרשות להגנת הפרטיות, וכן חברות ממשלתיות המהוות זרוע ביצועית של משרד התחבורה. שחקנים נוספים במגזר הציבורי הן רשויות מקומיות שאחראיות לתשתיות העירוניות ולתחום התחבורה באזורן, והן שותפות להכנסת מיזמים שונים בתחום התחבורה לשטח השיפוט שלהן במטרה לשפר את חיי האזרח. מעבר לכך, יש לציין את רשויות האכיפה, ביניהן המשטרה, אגף התנועה וגופי האכיפה הפועלים תחת הרשויות המקומיות. בנוסף, הוקמו גופים ציבוריים שונים בתחום התחבורה: התכנית הלאומית לתחליפי דלקים ותחבורה חכמה, קהילת Ecomotion, מכוני מחקר אקדמאים ומרכזי פיתוח שונים בחסות המדינה.

מגזר שירותים לרכב

מגזר זה כולל את כלל הגורמים העוסקים בייבוא, מכירה והשכרת רכבים (כולל שירותי ליסינג שונים), ואלו הנותנים שירותים "פיזיים" לבעלי רכבים, כגון תחנות דלק, מוסכים, ושירותי ביטוח.

מגזר תשתיות תחבורה

מגזר תשתיות התחבורה מתייחס לכלל הגורמים האחראים על התשתית הנדרשת לנסיעה ולהסעת המונים. השחקנים בתחום אחראים או מפעילים אלמנטים בדמות כבישים חכמים מרושתים בחיישנים, רמזורים ואמצעי ניהול תנועה, חניות פיזיות והפעלת חניה מרחוק, עמדות טעינת רכב חשמלי, כבישי אגרה וכן אמצעי בקרת שימוש ואמצעי גביה שונים הנדרשים לתשלום עבור שירותים אלה.

מגזר עסקי-טכנולוגי

מגזר זה כולל את חברות המידע והטכנולוגיה המספקות תשתית להפעלת אמצעים ושירותי תחבורה. סקטור זה כולל חברות תקשורת סלולרית, חברות המספקות תשתיות תקשורת פיזיות, ענקיות המידע כמו Google ו-Facebook, חברות מידע וטכנולוגיה וקהילת הסטארטאפים בתחום התחבורה.

מגזר תחבורה ציבורית ושיתופית

מגזר זה כולל את התחבורה הציבורית והתחבורה השיתופית. מגזר התחבורה הציבורית כולל את התחבורה המסורתית, כמו אוטובוסים, רכבות ומוניות ואת התחבורה החכמה: אוטובוס חכם, מפעילי מוניות דיגיטליים (Taxi Hailing), תחנות תחבורה ציבורית חכמות, מערכות המספקות מידע בנוגע לתחבורה הציבורית, וכן מערכות המאפשרות תשלום דיגיטלי עבור שירותי תחבורה כגון כרטיסי נסיעה חכמים (רב-קו), יישומוני תשלומים וארנקים דיגיטליים. נושא זה ידון בהרחבה בפרק 6 למדריך זה.

התחבורה השיתופית כוללת את חברות השכרת כלי הרכב לפי שימוש וכלי רכב זעירים דוגמת אופניים וקורקינטים. סקטור זה כולל גם פלטפורמות שיתוף נסיעות (Carpooling) ומערכות דיווח על עומסי תנועה וניתוב תנועת כלי רכב.

מגזר ציבורי
- ממשלתי
- תוכנית לאומית לתבורה
- רשויות מקומיות
- רשויות אכיפה

מגזר עסקי טכנולוגי
- חברות טכנולוגיה
- תשתיות מידע ותקשורת

מגזר שירותים לרכב
- רכבים
- שירותים

מגזר תחבורה ציבורית ושיתופית
- תחבורה ציבורית
- תחבורה שיתופית
- פלטפורמות
- אמצעי תשלום

מגזר תשתיות תחבורה
- כבישים
- חניה
- תשלומים

מגמות טכנולוגיות רלוונטיות ל'תחבורה חכמה' ולפרטיות משתמשים

רשת סלולרית דור 5 (5G)

הדור החדש של הרשתות הסלולריות (5G) מאפשר מהירות עיבוד גבוהה יותר של מידע, תעבורה רחבה יותר של נתונים וזמן השהייה נמוך יותר בעת העברתם. הטכנולוגיה תומכת במהירות גבוהה מג'יגה בייט לשנייה, ביחס לרשת 4G התומכת במהירות של כ-200 מגה בייט לשנייה, והיא הבסיס לתמיכה ברשתות של אלפי חיישנים, סנסורים ומצלמות הנדרשים לצורך הקמת תשתית לתחבורה חכמה.

Big Data: איסוף נתונים בלתי מוגבל

מושג ה- Big Data ניתן לאפיון בארבעה קריטריונים (4V's): נפח (Volume), מגוון (Variety), מהירות (Velocity) ואמיתות (Veracity). הטכנולוגיה מאפשרת אחסון ותעבורת נתונים מתקדמת בקצב אקספוננציאלי ומאפשרת אחסון גדול של נתונים ממגוון מקורות: טקסט, קול, תמונה, וידאו, מיקום, טמפרטורה, טביעות אצבע ועוד. חברות וארגונים משתמשים בנתונים שאספו על מנת להפיק תובנות ולהתאים את השירות הניתן ללקוח הקצה באופן מדויק ואישי ככל שניתן.

IoT: האינטרנט של הדברים, רישות המרחב הציבורי והפרטי בחיישנים

ה-IoT מיוחס לשימוש נרחב ויומיומי ברשתות, מצלמות, חיישנים ומחשבים מקושרים המוטמעים בתוך חפצים, עצמים קיימים ופרטי לבוש. לכל מכשיר זיהוי ייחודי ואפשרות להעביר מידע ברשת לחיישנים ומחשבים אחרים ללא אינטראקציה אנושית. מערכות אלה מאפשרות יכולות זיהוי, איסוף וניתוח נתונים, הסקת מסקנות, קבלת החלטות וביצוע פעולות באופן עצמאי.

התפתחויות מרכזיות בעולם התחבורה

MaaS: פלטפורמות ניידות כשירות (Mobility as a Service)

מעבר מרכישת מוצרים לרכישת שירותים היא מגמה צרכנית המתאפשרת באמצעות יכולות טכנולוגיות. צריכת שירותים לפי צורך (On Demand) בזמן ובמידה הנדרשים ותשלום לפי שימוש מגבירים את הנגישות לאמצעי התחבורה השונים תוך מקסום יעילות השימוש בהם. לדוגמה, שימוש ברכבים שיתופיים כתחליף לרכישת רכב במידה והצורך הוא ממוקד ומינימלי. ההערכה היא שמכונית בבעלות פרטית אינה נמצאת בשימוש כ-95% מהזמן, ורוב המושבים בה נותרים ריקים בזמן נסיעה. פלטפורמות הניידות כשירות, מאפשרות ייעול וצמצום השימוש ברכב פרטי. חשוב לציין כי השימוש בפלטפורמות מקדם אמצעי תשלום חדשים, ארנקים וירטואליים והעברות דיגיטליות, הדורשים אימות פרטים ושואבים נתונים נוספים מלקוחות.

קיימים שלושה מודלים מרכזיים בתחום שירותי הנסיעות: **מודל שיתוף רכב** (Car Sharing), המתייחס לאפשרות שכירת כלי תחבורה מאדם פרטי באמצעות פלטפורמה דיגיטלית, בתשלום לפי זמן שימוש או לפי נסיעה. **מודל שיתוף נסיעות** (Ride Sharing), המתייחס למצב בו אנשים פרטיים נוסעים יחדיו ברכב בנסיעה משותפת (Carpooling), באופן שמנצל את המושבים הריקים ברכב. שלישי הוא **מודל שירותי נסיעה**, שמתייחס לשימוש פרטים בחברות המספקות שירותי הזמנת רכב (Ride-Hailing) לנסיעה אישית (בדומה למונית) או להסעה משותפת (שכוללת איסוף נוסעים נוספים). השירותים גמישים במחיר ובמסלול, ונקבעים לפי היצע וביקוש ממוקד.

P2P (עמית לעמית): פלטפורמות לשירותים מבוזרים

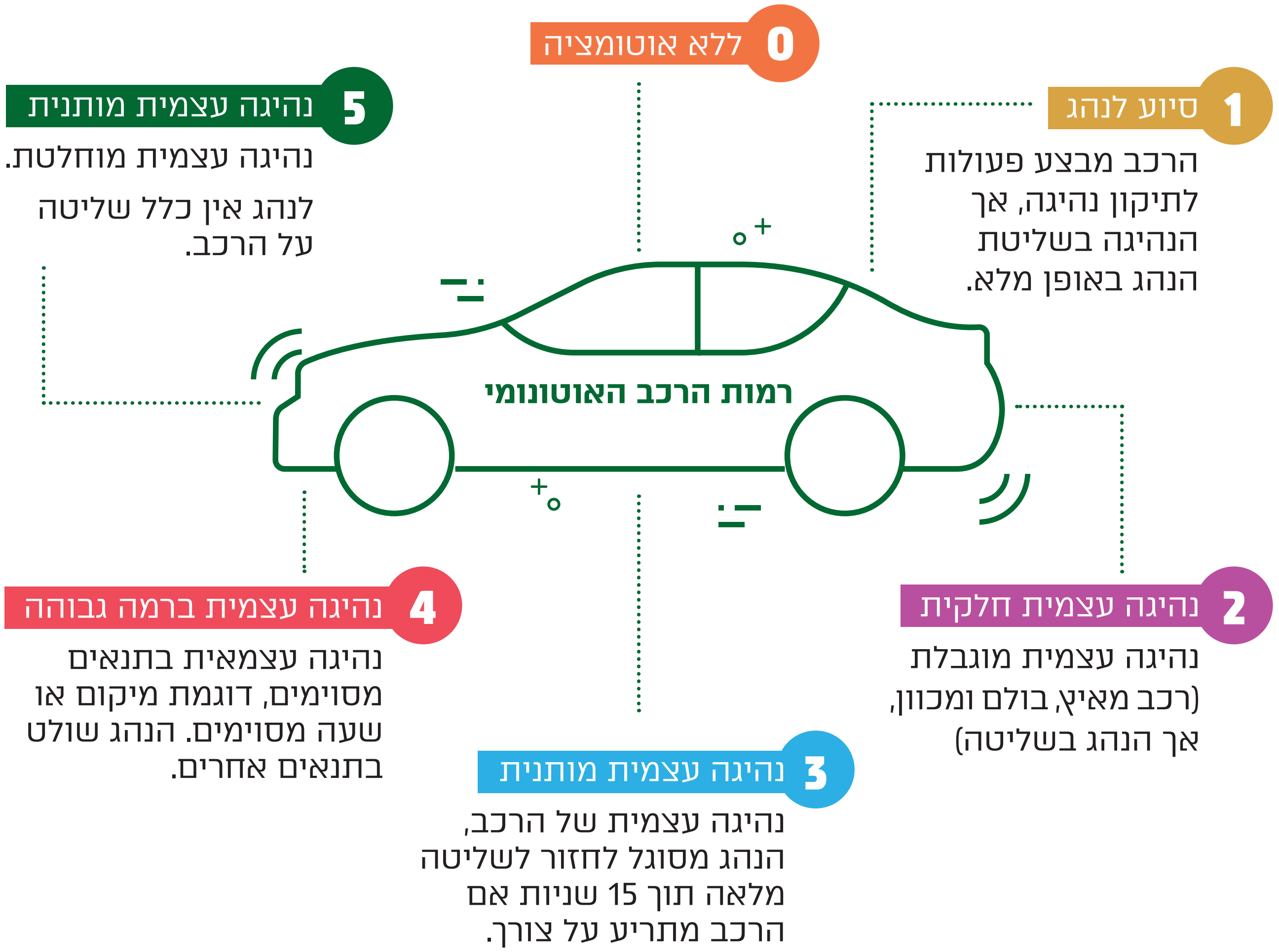
מושג זה מיוחס לכלל תשתיות הטכנולוגיות שמהוות פלטפורמה לצרכנים לספק ולצרוך שירותים שונים אחד מהשני בתחום התחבורה. הפלטפורמה מאפשרת לכל אדם לספק שירותי תחבורה במסגרתה, ולאדם אחר לצרוך שירותים אלו לפי צורך (On Demand). הפלטפורמות מגדילות את ההיצע הקיים ומוזילות את עלות השירותים. כך לדוגמה, Uber מאפשרת לעשרות אלפי בעלי רכב פרטיים לספק שירותים שבעבר סופקו על ידי שירותי מוניות.

Last Mile: הק"מ האחרון לנסיעה

מושג זה מיוחס למגמת ההתפתחות של תחום פתרונות התחבורה המספקים מענה תחבורתי לטווח הקצר, בהם מיקרו-ניידות (Micro Mobility). בהקשר זה ניתן לציין את כלי הרכב הזעירים, כגון קורקינטים ואופניים חשמליים, המספקים שירותי תחבורה אזוריים לפי צורך המשתמש, ומאפשרים ניידות ללא תחנות או קו מוגדר, וזאת על פי רוב בהפעלה עצמית.

ACES: רכב אוטונומי, מקושר, חשמלי ושיתופי

מושג זה מיוחס למהפכת הרכב העתידי. כיום נהוג להבחין בין ארבעה סוגי רכבים. **רכב חשמלי** הפועל על תחליפי דלקים, שצורך אנרגיה נקיה יותר; **רכב שיתופי**, שנמצא בבעלות משותפת או שמבוצע בו שימוש לפי דרישה על ידי מספר אנשים; **רכב מקושר**, רכב המקושר באמצעות רשתות חיישנים ומצלמות לסביבתו ולרכבים נוספים וכן לרשתות תקשורת ומאפשר נסיעה יעילה ובטוחה יותר; **והרכב האוטונומי**, בעל מסוגלות לנסיעה עצמאית ברמות שונות (רמה 0 ללא אוטומציה כלל ועד רמה 5 לנהיגה עצמית מוחלטת שאינה בשליטת הנהג, כשבין שתי הרמות ישנו סיוע לנהג, הכוונה, תיקוני נהיגה, הכוונה ועד נהיגה עצמאית שיכולה לחזור לנהג בתנאים מסוימים). רכבים חדשים מסוגים אלה מרושתים בחיישנים הקולטים מידע מתוך הרכב ומחוצה לו, ואוגרים כמות נתונים בסדרי גודל משמעותיים.



איסוף ושיתוף מידע: בסיס לתכנון, פיקוח ופיתוח השוק

משרדי ממשלה ורגולטורים מודעים לערך הקיים במאגרי מידע פתוחים ונגישים (Open Databases) לציבור ולמשק. התפיסה המקובלת כיום היא שעל ידי הסדרת מאגרי מידע ושיתוף נתונים ניתן לייצר שיתופי פעולה ולקדם שירותים שונים בסביבה העסקית. לאור האמור, בימים אלה פועל משרד התחבורה על טיוב מאגרי מידע קיימים המכילים נתונים של גופי התחבורה הציבורית בזמן אמת, וכן פועל לגיבוש סטנדרט אחיד לשיתוף מידע תחבורתי לשם תכנון מיטבי של תחבורה ציבורית.

מערכות ניהול ובקרת תנועה: אופטימיזציה בכבישים

אופטימיזציה בכבישים הינו מושג המיוחס למגמה של פיתוח והטמעה של מערכות בקרת תנועה לעיבוד נתונים באמצעות רשת מצלמות, חיישנים, רמזורים ואמצעים נוספים לשם ויסות אופטימאלי של זרימת התנועה. מעבר לכך, המידע הנאסף יאפשר זיהוי אתגרים וכשלים תחבורתיים ויסייע בחשיבה על פתרונות בשיתוף הסביבה העסקית. בימים אלה פועלים ומוקמים מרכזי ניהול תנועה במטרופולינים הגדולים במדינה: ירושלים, תל אביב וחיפה.

פרק 2 | פרטיות

הזכות לפרטיות על קצה המזלג

הזכות לפרטיות היא זכות יסוד חוקתית אשר נקבעה בחוק-יסוד: כבוד האדם וחירותו. סעיף 7 לחוק היסוד קובע, בין השאר כי "כל אדם זכאי לפרטיות ולצנעת חייו". בהמשך, מפרט החוק מהי פגיעה בפרטיות על ידי ציון מספר מצבים של פגיעה בפרטיות, כמו כניסה לרשות היחיד של אדם שלא בהסכמתו. יחד עם זאת, הזכות לפרטיות אינה זכות מוחלטת, והפגיעה בה כפופה לעמידה במבחנים משפטיים מסוימים.

נוסף על מעמדה של הזכות לפרטיות כזכות יסוד חוקתית, נהנתה הזכות עוד לפני חקיקת חוק היסוד, להגנה מפורשת ונרחבת בחוק הגנת הפרטיות, התשמ"א-1981. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות מהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית שעונשה עד חמש שנות מאסר. אחד מעקרונות הבסיס של החוק הוא דרישת ההסכמה. החוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו" וכי הסכמה צריכה להיות מדעת, ולהינתן במפורש או במכללא.

הכלל הוא שאין לאסוף מידע על אדם אלא אם הוא מודע שמידע נאסף אודותיו, הוא מסכים לאיסוף המידע וכן מסכים לשימושים השונים שאוסף המידע מבקש לעשות בו.

פרק ב' לחוק מתמקד בהגנה על מידע אישי, וקובע משטר הגנה על הזכות לפרטיות במאגרי מידע – להרחבה ראו פרק 4 למדריך זה העוסק בנושא.

מכוח החוק הותקנו תקנות וצווים בעניינים שונים, ובהם תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן – 'תקנות אבטחת מידע'), המסדירות את חובות אבטחת המאגר החלות על בעל מאגר מידע, מנהל המאגר והמחזיק בו.

הרשות להגנת הפרטיות

הרשות להגנת הפרטיות (להלן: 'הרשות') הינה הגוף המסדיר, המפקח והאוכף את הוראות חוק הגנת הפרטיות על כלל הגופים בישראל - פרטיים, עסקיים או ציבוריים, המחזיקים או מעבדים מידע אישי באופן דיגיטלי.

במסגרת תפקידה כרגולטור של דיני הגנת הפרטיות ודיני הגנת המידע הרשות מופקדת על הגנת המידע האישי המוחזק במאגרי מידע כהגדרתם בחוק הגנת הפרטיות, ועל ביצורה של הזכות לפרטיות. הרשות פועלת להשגת מטרה זו באמצעות התוויית מדיניות, אסדרה, הדרכות, אכיפה מנהלית, אכיפה פלילית ופיקוחי רוחב (Audit).

הרשות היא שמתווה את מדיניות ההגנה על המידע האישי במאגרי מידע דיגיטליים. משימותיה המרכזיות של הרשות הן קידום שליטת הפרט במידע אישי על אודותיו, השפעה על תהליכי 'עיצוב לפרטיות' בארגונים ובמערכות מידע בכל מגזרי המשק והגברת תחושת המוגנות ותחושת הביטחון של הציבור ביחס למידע האישי המוחזק במאגרי המידע. כל זאת, במטרה לצמצם את הסיכונים הגוברים לפגיעה בפרטיות בעת החזקת מידע דיגיטלי, בעיבודו או בניהולו, והכל תוך איזון ומתן משקל ראוי לחידושים הטכנולוגים וליתרונותיהם עבור השוק וקהל המשתמשים.

הרשות להגנת הפרטיות רואה כמשימתה העיקרית קידום של ציות לדיני הגנת המידע בכל ארגון, עסק וגוף פרטי או ציבורי המחזיקים במידע אישי, כך שיפעלו לניהול המידע שברשותם באופן תקין בהתאם לדיני הגנת הפרטיות.

פרק 3 | אתגרי הפרטיות בתחבורה החכמה

סביבת התחבורה, ובעיקר התחום הטכנולוגי בה, מתפתחת בקצב מהיר. שחקנים שונים מפתחים ומקדמים פתרונות תחבורה חכמים, הן בתחום התשתיות והכלים הפיזיים והן בתחום הפלטפורמות והשירותים הדיגיטליים. כפי שצוין, המגמות הטכנולוגיות, רישות סנסורים (IoT) ויכולת תעבורת המידע (Big Data), מאפשרות התפתחות זו תוך הישענות על מידע אישי ונתונים רבים שחלקם שייך למשתמשים בשירות או לתושבים שנמצאים בסביבתו.

להפעלת השירותים ישנן השלכות על פרטיות המשתמשים המצריכות התייחסות. ראשית, המרחב הציבורי ותחום השירותים המתקדמים עוברים למצב בו ה**משתמש יהיה נתון תחת מעקב** תמידי שיבוצע על ידי רשתות של מצלמות וחיישנים שונים שיופעלו על ידי רכבים, אפליקציות המותקנות על הטלפון הסלולרי האישי, תשתיות חכמות ואמצעים לניהול התנועה והמרחב העירוני. **שנית, מלבד השימוש הראשי בנתונים למטרה לשמה נאספו, עומדים הנתונים בפני סיכון לשימוש** משני, כגון ניתוח פרטי משתמשים, יצירת פרופילים, ניתוח העדפות **ולמידה סטטיסטית של התנהגות המשתמשים והציבור בכללותו.**

המתח המרכזי שנוצר הוא **בין מתן שירותי תחבורה חכמה לבין מעקב ופגיעה בפרטיות המשתמשים.** המשתמשים מוסרים מידע אישי לצורך קבלת שירות טוב יותר ומותאם אישית. ואולם, משמעות הדבר היא, בין היתר, פגיעה בפרטיותם. בסקר שביצעה הרשות להגנת הפרטיות בנושא הפרטיות בתחום התחבורה 40% מהמשתתפים ציינו כי הם לא יסכימו למסור מידע אישי על מנת לקבל שירות טוב יותר בתחבורה, לעומת 44% שציינו כי הם יסכימו למסור מידע אישי באופן חלקי בלבד (נתוני הסקר מופיעים בסוף פרק זה). נתונים אלו מעידים על המתח הקיים בין הצורך להעניק שירותי תחבורה יעילים לבין הפגיעה בפרטיותם של המשתמשי בפרט, והציבור הישראלי בכלל, ועל הצורך למצוא איזון ראוי בין הדברים.

אתגרי פרטיות מרכזיים בתחום התחבורה:

1. שימוש במאגר המידע בכפוף לעקרון צמידות המטרה – הפעלת שירותי תחבורה מצריכה החזקה במאגרי מידע עם מידע אישי רב, כגון: פרטי לקוחות, פרטי התקשרות, פרטי תשלום, נתוני שימושים, היסטורית פעולות ותשלומים ועוד. עקרון צמידות המטרה קובע שכל שימוש במידע ייעשה אך ורק בהתאם למטרה שלשמה המידע נאסף מלכתחילה.

2. **איסוף נתונים עודף** – מספר החיישנים שנפרסים ע"י גופי התחבורה גדל בקצב מהיר. פריסה זו מאפשרת איסוף נתונים מופרז ביחס למה שנחוץ להשגת המטרה. תופעה זו מתעצמת עם הוספת פונקציות רבות, שירותים וממשקים הנמצאים בתוך כלי הרכב ובפרט בכלי רכב מחוברים.

3. **אבטחת מידע** – נתונים אישיים המאוחסנים בכלי רכב או במקומות חיצוניים (למשל, בתשתית מחשוב ענן של גוף התחבורה) עלולים להיות לא מאובטחים כראוי ובכלל זה לא מאובטחים מפני גישה לא מורשית (למשל, במהלך תחזוקת הרכב).

4. **דיוור ישיר** – תחום הדיוור הישיר ללקוחות (או לקוחות פוטנציאלים) מוגדר בחוק הגנת הפרטיות ובחוק התקשורת (בזק ושידורים), התשמ"ב-1982 ("חוק הספאם"). הפרסום הממוקד מעניק ערך לארגון וללקוח אך דורש עמידה בתנאים ברורים המפורטים בחוק, ובראשם קבלת הסכמה מנושא המידע לקבל הודעות בדיוור הישיר.

5. **פרטיות כחסם עסקי** – הרגולציה ועקרונות הפרטיות מגדירים את מסגרת העבודה והדרישות שיש לקיים בעת השימוש במידע אישי של לקוחות. יש הטוענים כי דיני הגנת הפרטיות עלולים להכביד על הארגונים השונים וליצור חסמים להתפתחויות טכנולוגיות ועסקיות שונות. על מנת להתמודד עם חשש זה יש להבין את דרישות החוק ואופן יישומן וזאת על מנת לאפשר קבלת החלטות מבוססת מידע (Data Driven Decision) תוך שמירה על פרטיות המשתמשים.

6. **עיצוב לפרטיות (Privacy by Design)** – על מנת לעמוד בדרישות החוק, בין אם בשוק המקומי או בשוק הגלובלי, מומלץ כי החברות יעמדו בדרישות שונות להגנת הפרטיות, לרבות ההמלצה לעיצוב לפרטיות. לפי עיקרון זה, וכדי שספק שירות לא יתקל בחסם עסקי או מגבלות בשלב מתקדם של פיתוח השרות, מומלץ שהספק יטמיע את עקרונות הפרטיות כבר בשלב תכנון המוצר או השירות.

7. **מכרזים וחוזים** – נושא הפרטיות אינו מקבל התייחסות מפורטת במכרזים ובחוזים, בעיקר של גופים ציבוריים. ברוב המקרים מנסח המכרז מסתפק בסעיף המורה על החובה לעמוד בהוראות החוק להגנת הפרטיות ללא כל פירוט נוסף מעבר לכך. יש לפעול לעמידה בהוראות תקנה 15 לתקנות אבטחת מידע ובהוראות הנחיית הרשות בעניין שימוש במיקור חוץ לעיבוד מידע אישי, ולהטמעת דרישת העיצוב לפרטיות' בחוזי ההתקשרות והמכרזים של הגופים הציבוריים כדי להביא לקיום אופטימלי של הוראות החוק והתקנות על ידי נותני השירותים.

8. **ריבוי נותני שירותים ופיזור המידע** – שוק התחבורה החכמה הינו שוק תחרותי הכולל שחקנים רבים המספקים שירותים שונים ומגוונים. בשוק הקיים, על מנת להשתמש בצורה סבירה ומספקת בשירותי התחבורה הציבורית והשיתופית, משתמשים נדרשים למסור פרטים אישיים, פרטי אמצעי תשלום ולהתיר למספר רב של חברות לעקוב אחר התנהלותם. דרישות אלו מייצרות חשש בקרב משתמשים לשימוש לא ראוי בנתונים הנוגעים אליהם על-ידי גופי התחבורה.

9. **פערי ידע –** חברות וארגונים נתקלים בקשיים ביישום הוראות חוק הגנת הפרטיות והתקנות. לאור האמור, נוצר פער בין הרצון לקיים את הוראות החוק והתקנות לבין היישום דה-פקטו של הוראות אלה בשל היעדר ההבנה והידע כיצד ליישם אותן. כך לדוגמה, חברות שונות עשויות להיתקל בשאלות כגון מהי מידת אבטחת המידע החלה על מאגרי המידע שלהן או באיזה אופן עליהן לנהל את מאגרי המידע שבבעלותן.

פרק 4 | החובות הכלליות ביחס לאיסוף ולשימוש במידע אישי

פרק זה מפרט את הדרישות הבסיסיות לפי חוק הגנת הפרטיות בעניין איסוף ושימוש במידע אישי במאגרי מידע. דרישות אלה רלוונטיות הן ביחס לטכנולוגיות המשמשות את גופי התחבורה והן ביחס למאגרי המידע הנוצרים במסגרת השימוש בטכנולוגיות האמורות.

ניהול מאגרי מידע

בגופי התחבורה **מצטברת כמות עצומה של מידע אישי ממקורות ומאגרים שונים**, החל ממאגרים בסיסיים המכילים מידע כללי על תושבי המדינה ועד מאגרים ייחודיים כמו מאגרי מידע של רשת ה-WiFi העירונית, מאגר כרטיסי הנסיעה החכמים (כגון רב קו) או מאגרי אפליקציות תחבורה שונות. לעיתים קרובות, המידע נאסף ונאגר על ידי גורמים חיצוניים וקבלני משנה. היקף המידע הרב הזה מחייב את גופי התחבורה לנהלם בצורה מאובטחת, תוך הקפדה על ניהול מאגרי מידע קפדני ויישום תקנות אבטחת מידע על מנת למנוע זליגת מידע אישי.

בפרק ב' לחוק, נקבעו הוראות לעניין הגנה על הפרטיות במאגרי מידע, בין היתר בהיבטי חובת הרישום של מאגר המידע אצל רשם מאגרי המידע (הרשות להגנת הפרטיות), אופן החזקת מאגר המידע, אבטחת מאגר המידע, חובות בעל המאגר ומנהל המאגר, זכויות נושאי המידע - האנשים שמידע אודותיהם נאסף ונשמר במאגרי המידע וכן השימושים המותרים במידע השמור במאגרי המידע השונים:

1. **חובת הרישום –** בהתקיים אחד התנאים בסעיף 8(ג) לחוק, נדרש בעל מאגר מידע לרשום את המאגר אצל רשם מאגרי המידע (הרשות להגנת הפרטיות).
2. **עקרון צמידות המטרה –** מחובתו של גוף תחבורה לעמוד בעקרון 'צמידות המטרה' ולעשות שימוש במידע אך ורק לטובת המטרה שלשמה הוא נאסף ולא לשם אף מטרה אחרת (סעיף 8(ב)).
3. **חובת מתן הודעה –** גוף תחבורה המבקש לאסוף מידע ממשתמש, להחזיק או לעשות בו שימוש, מחויב ליידע את המשתמש בטרם איסוף המידע הנוגע אליו, האם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו והסכמתו, מהי המטרה שלשמה מבוקש המידע, ולמי יימסר המידע (סעיף 11 לחוק).

4. **זכות עיון במידע –** חובת גוף תחבורה לאפשר לכל משתמש לעיין במידע אודותיו המוחזק במאגר המידע, וזאת תחת מספר מגבלות המפורטות בסעיף 13 לחוק).
5. **זכות תיקון המידע –** נושא המידע רשאי לדרוש תיקון של מידע אודותיו, ככל שהמידע במאגר אינו נכון, שלם, ברור או מעודכן (סעיף 14 לחוק).
6. **חובת הסודיות –** בעל מאגר המידע, הגורם המחזיק במאגר ומי מעובדיהם, מחויבים בשמירת סודיות המידע אליו נחשפו כחלק מעבודתם (סעיף 16 לחוק).
7. **בעת פנייה בדיוור ישיר,** מחויב גוף התחבורה להקפיד על עמידה במספר כללים הנגזרים מחוק הגנת הפרטיות ומובאים בהרחבה בהנחית רשם מאגרי המידע מספר 2/2017 פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר שירותי דיוור ישיר.
8. **חובת אבטחת המידע –** בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע (סעיף 17 לחוק) וכן עמידה בתקנות אבטחת מידע.

דוגמה

מפעיל שירותי השכרת אופניים באמצעות אפליקציה מחזיק במאגר מידע של לקוחות השירות. במסגרת השימוש נדרשים לקוחות להירשם באמצעות טופס הרשמה. מאגר המידע כולל נתונים של כ-14,000 משתמשים באזור ההפעלה, וכוללים את נתוני הלוקחות ואת היסטוריית הנסיעות שלהם. בנוסף, מידי תקופה שולח המפעיל דיוור ישיר באמצעות מסרון או מייל ללקוחות בנושאים שונים.

מפעיל השירות מחויב **ברישום מאגר המידע** מכיוון שעומד בשני תנאים, למעלה מ-000,01 אנשים ומאגר לצורך דיוור ישיר. הרישום במאגר מחייב **אישור וקבלת הסכמה של הלקוחות הנרשמים תוך ציון מטרת המאגר ושימוש לטובת מטרה זו בלבד.**

כמו כן המפעיל מ**חויב בשמירת סודיות המידע ובמתן אפשרות לעיון בפרטי מידע** אישיים על ידי לקוחות. בנוסף, אין באפשרותו להעביר את הפרטים לצד שלישי **או להשתמש בהם למטרה אחרת שלא צוינה,** למעט אם קיבל אישור מפורש מנושאי המידע (הלקוחות).

תקנות הגנת הפרטיות (אבטחת מידע)

ריבוי המידע המצטבר במאגרי מידע של גופי תחבורה מחייב, כאמור, ניהול של המידע בצורה מושכלת והקפדה, בין היתר, על אבטחת המידע הנאסף. תקנות אבטחת מידע מפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות הישראלי על כל גורם המחזיק או מנהל מאגר מידע. התקנות חלות על כלל המשק הישראלי והן קובעות מנגנונים ארגוניים ודרישות מהותיות שמטרתן הפיכת אבטחת המידע לחלק משגרת הניהול השוטף של הארגון.

בפרק זה מובאים בתמצית העקרונות המרכזיים של אבטחת המידע במאגרי מידע של גופי תחבורה, בהתאם לחובות המפורטות בתקנות אבטחת מידע. גופי תחבורה מחויבים להקפיד על יישום עקרונות אלה באופן שוטף, וכן בטרם הטמעת טכנולוגיות ומיזמים שונים.

מחובת כל גוף תחבורה להגדיר מהי **רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותו. בהתאם להגדרת רמת האבטחה החלה על המאגר, יבחן גוף התחבורה אילו הוראות בתקנות חלות על המאגר. כך למשל, רמת האבטחה הגבוהה תחול על מאגר המכיל מידע אודות 100,000 אנשים ומעלה, או שמספר בעלי ההרשאה לעיון ופעולות בו עולה על 100 מורשים וזאת ביחס למאגר אשר מטרתו העיקרית היא לשירותי דיוור ישיר, או שהוא כולל מידע הנוגע לצנעת חייו האישיים של אדם; מידע רפואי או מצב נפשי; מידע גנטי; עמדות פוליטיות או אמונות דתיות; עבר פלילי; נתוני תקשורת; נכסים והתחייבויות כלכליות והרגלי צריכה של אדם אשר יש בהם ללמד על מידע כאמור.**

בהמשך, לאחר שנבדקה והוגדרה רמת האבטחה הנדרשת למאגר המידע, יש לפנות לטבלת הסבר המפרטת אילו תקנות חלות על המאגר.

להלן מובאות בתמצות התקנות המרכזיות הרלוונטיות למאגרים:

1. **חובת גוף תחבורה לנהל 'מסמך הגדרות מאגר'**, לכל מאגר בכל רמת אבטחה, וזאת בהתאם לתקנה 2 לתקנות אבטחת מידע. על בעל מאגר מידע לבחון את הצורך בעדכון המסמך אחת לשנה לפחות ובכל פעם שנעשה שינוי משמעותי, כמפורט בתקנה. המסמך יכלול: **תיאור כללי** של פעולות האיסוף והשימוש במידע, **תיאור מטרות איסוף המידע, תיאור סוגי המידע** השונים הכלולים במאגר, פרטים על העברת מאגר המידע או שימוש מחוץ לגבולות ישראל (למשל: המידע אינו מעובר לחו"ל ומעובד במאגרים המצויים על שרתי גוף התחבורה). האם נעשה **עיבוד באמצעות גורם זר או חיצוני** (לדוגמא: על אף שהמאגר מוחזק בשרתי גוף התחבורה, המיזם ופלטפורמת עיבוד המידע מופעלות על ידי חברת "XYZ", המשמשת כספק חיצוני בהסכם), **מיפוי סיכונים** אפשריים ודרכי התמודדות עמם, פרטים אישיים של מנהל המאגר, מחזיק המאגר וממונה אבטחת המידע.
2. **חובת גוף תחבורה למנות ממונה אבטחת מידע**, כנדרש בסעיף 17ב (א) לחוק, בהתאם לתנאים המפורטים בתקנה 3. תנאים ודגשים ספציפיים מובאים בהרחבה במדריך תקנות

הגנת הפרטיות (אבטחת מידע) שפרסמה הרשות להגנת הפרטיות.

3. **חובת גוף התחבורה לקבוע, במסמך ברור, נוהלי אבטחת מידע, שמטרתם לייצר מדיניות אבטחת מידע עקבית בארגון,** כך שניתן יהיה להתמודד עם סיכוני אבטחה אליהם חשוף המידע. חובה זו מעוגנת בתקנה 4.

4. **גוף התחבורה מחויב לבצע מיפוי של מערכות המאגר הנמצאות בבעלותו/החזקתו וכן סקר סיכונים.** כלומר, על גוף התחבורה להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת פרטים כמו: תשתיות ומערכות חומרה, סוגי רכיבים, תוכנות, ממשקים וכן פרטים נוספים המובאים בהרחבה בתקנה 5. **מאגר עליו חלה רמת האבטחה הגבוהה מחויב לערוך סקר לאיתור סיכוני אבטחת מידע** (סקר סיכונים) **אחת ל-18 חודשים לפחות** ולפעול לתיקון ליקויים, אם התגלו. כמו כן, על מאגרים אלה חלה חובה לבצע **מבדקי חדירות** אחת ל-18 חודשים לפחות, לבחינת עמידותם.

5. **חובת גוף התחבורה להגן פיזית על תשתיות החומרה המשמשות את המאגר**, במקום מוגן המונע כניסה ללא הרשאה. כמו כן, גוף התחבורה מחויב לתעד כניסת ויציאת **עובדים מאתרים בהם מצויות המערכות** (מצלמות, זיהוי ביומטרי וכד'), כמפורט בתקנה 6 לתקנות.

6. **גוף התחבורה מחויב למזער את הסכנה הפוטנציאלית שמציב הגורם האנושי** באמצעות העסקת עובדים אשר עברו הכשרות מתאימות בתחומי אבטחת המידע. בנוסף, **מחובת גוף התחבורה לבחון את מידת התאמתם של העובדים הקיימים ולהעביר הדרכות אחת לשנתיים**, לכל הפחות. בתוך כך, על גוף התחבורה לנהל הרשאות גישה למאגריה בצורה מסודרת ואחראית, כמפורט בתקנות 7 ו-8.

7. **גוף התחבורה מחויב לוודא שעובדים להם קיימת גישה למאגר הם אכן עובדים מורשים לכך, וזאת באמצעות זיהוי ואימות** (לכל הפחות באמצעות סיסמא). כמו כן, נדרש לנהל מנגנון המתעד באופן אוטומטי ועצמאי כל גישה למערכת, עליו תבוצע בקרה תקופתית, כמפורט בתקנות 9 ו-10.

8. **חובתו של גוף התחבורה לתעד את כל אירועי האבטחה שהתרחשו, על מנת לייצר זיכרון ארגוני ביחס לאירועים חריגים ולהפיק מהם לקח לעתיד.** תקנה 11 לתקנות מגדירה מהו 'אירוע אבטחה חמור' כשמדובר במאגר עליו חלה רמת האבטחה הגבוהה ומהו אותו אירוע כשמדובר ברמת אבטחה בינונית. במקרה של "אירוע אבטחה חמור" כהגדרתו בתקנות, **מחויב גוף התחבורה להודיע לרשות להגנת הפרטיות באופן מידי על כך**, וכן לדווח על הצעדים שננקטו בעקבות האירוע. ניתן לדווח באופן מקוון באתר האינטרנט של הרשות.

9. **גוף התחבורה מחויב להקפיד על מניעת זליגת מידע בעת שימוש בהתקנים ניידים** (מחשבים ניידים, טלפונים חכמים וכד'), במידת הצורך באמצעות הגבלת חיבור המאגרים להתקנים ניידים (תקנה 12). כמו כן, **יש להקפיד על ניהול מאובטח ומעודכן של מערכות המאגר** (תקנה 13). בנוסף, במידה ומערכות המידע והמאגרים מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, **מחובת גוף**

התחבורה לנקוט באמצעי אבטחה נוספים שימנעו גישה חיצונית ולא מורשית למידע (תקנה 14).

10. **חובת גוף התחבורה לנקוט משנה זהירות כאשר מוענקת גישה למאגרי המידע לגורמים חיצוניים בהתקשרות באמצעות מיקור חוץ (כמפורט להלן בהתייחסות לתסקיר בפרק 5 במדריך זה). עוד בטרם התקשרות במיקור חוץ** על גוף התחבורה לבחון את סיכוני אבטחת המידע האפשריים, ובמידה והם גבוהים מידי יש להימנע ממיקור חוץ (ראו פירוט בפרק 5 למדריך זה). כמו כן, יש לקבוע בהסכם מפורש עם הספק החיצוני קווים מנחים לפעילותו, בין היתר: סוג המידע אותו רשאי לעבד, מערכות אליהן רשאי לגשת, חובתו לסודיות ועוד (כמפורט בתקנה 15 וכן בהנחיית רשם מאגרי מידע מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי).

11. **גוף התחבורה מחויב לערוך ביקורת פנימית או חיצונית, אחת ל-24 חודשים לפחות**, באמצעות גורם בעל הכשרה מתאימה, שאינו הממונה על אבטחת המאגר מטעמה, וזאת על מנת לוודא עמידה בתקנות, כמפורט בתקנה 16. ניתן לבצע את הביקורת במסגרת עריכת סקר סיכונים (כמוסבר בתקנה 5).

12. **גוף התחבורה מחויב להקפיד על משך זמן שמירת נתוני האבטחה ועל גיבוי ושחזור נתוני אבטחה**, שיש לבצע אחת לתקופה ובהתאם לדגשים המובאים בתקנות 17-18.

13. חשוב לזכור כי **חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר** על בעל המאגר, על מנהל המאגר ועל המחזיק במאגר (סעיף 17 לחוק). כמו כן, לרשות להגנת הפרטיות שמורה הזכות לפטור מאגרים ספציפיים מחובות אבטחת מידע מתוך התקנות, או לחלופין להטיל חובות נוספות בהתאם לנסיבות, כמפורט בתקנה 20.

מידע נוסף בנושא, ובכלל זה מדריך שאלות ותשובות בנושא תקנות אבטחת מידע ניתן למצוא באתר הרשות להגנת הפרטיות

פרק 5 | עקרונות להטמעת טכנולוגיות חדשות

בפרק הקודם הוצגו העקרונות המחייבים הבסיסיים בחוק הגנת הפרטיות בנוגע לאיסוף ושימוש במידע אישי. עקרונות אלה מחייבים גם ביחס לטכנולוגיות מידע המצויות בשימוש בגופי תחבורה ולמאגרי המידע הנוצרים תוך כדי השימוש בהן. **בפרק זה נפרט עקרונות נוספים אותם מומלץ לגוף התחבורה ליישם כדי להתמודד עם הסיכונים המוגברים לפרטיות – סיכונים הנובעים מן המאפיינים הייחודיים של שימוש בטכנולוגיות מידע,** אשר תוארו והודגמו בפרקים הקודמים למדריך. יודגש כי אין באמור בפרק זה בכדי להצביע על עמדת והמלצת הרשות להגנת הפרטיות ביחס לטכנולוגיות מסוימות.

מומלץ שגוף התחבורה יפעל בהתאם לעקרונות אלו בטרם מתקבלת החלטה על שימוש במיזם דיגיטלי חדש או על רכישה של טכנולוגיה או מערכת מידע חדשה. המלצתנו היא לקרוא עקרונות אלו כמבוא לדפי המידע הספציפיים בנושאים ובטכנולוגיות שהרשות להגנת הפרטיות תפרסם ותעדכן מעת לעת.

אחד מיסודות הניהול הנכון של טכנולוגיות תחבורה טמון בהפנמה מוקדמת של שיקולי פרטיות באמצעות "האחריותיות" (Accountability) וגישה מתכללת. **מומלץ שגוף התחבורה ינקוט באמצעים ארגוניים, טכנולוגיים ומשפטיים שישפרו את מידת ה"אחריותיות" והמחויבות שלו לצמצום ההשלכות של הטכנולוגיה על פרטיות המשתמשים.** מדובר באמצעים שהפכו לפרקטיקה מקובלת בגופי תחבורה בעולם, ובמקומות רבים כגון באיחוד האירופי, גם מכוח דרישה חוקית ורגולטורית מפורשת. גם בישראל, ללא יישום עקרון האחריותיות, לא יצליח גוף התחבורה, שהוא רשות ציבורית או ספק של רשות ציבורית, להגן על הזכות החוקתית של משתמשים לפרטיות, ויתקשה להימנע מפגיעה בפרטיותם במידה העולה על הנדרש.

ניהול מתכלל

1. ראשית, מומלץ למנות בגוף התחבורה גורם בכיר שיהיה אחראי לקביעת מדיניות כוללת בעניין השימוש במיזמי טכנולוגיות מידע ויתכלל את הטיפול בהם. בעידן ניתוחי ביג דאטה וטכנולוגיות בינה מלאכותית, סיכוני הפרטיות נובעים לא רק מהמאפיינים של כל פרויקט טכנולוגי בפני עצמו – אלא גם מהשפעות הגומלין בין הטכנולוגיות השונות ומהצלבת המידע הנאסף תוך כדי הפעלתן במקביל. לכן, נדרשת יד מכוונת ונקודת מבט מערכתית לשם הערכה מדויקת של הסיכונים לפרטיות והטיפול בהם.
2. במידה וקיים בגוף התחבורה 'ממונה על הגנת הפרטיות' (DPO), מומלץ שגורם זה יהיה אחראי על המשימה. 'ממונה הגנת הפרטיות' הוא תפקיד שונה מ'ממונה אבטחת המידע' שעל פי הוראות חוק הגנת הפרטיות קיימת חובה למנות בגופים ציבוריים ובארגונים נוספים. 'ממונה הגנת הפרטיות' הוא לרוב נושא משרה בכיר המרכז ועוסק בכל הצדדים המשפטיים של הגנת המידע האישי בגוף התחבורה, ובמידת הצורך מנחה גם את ממונה האבטחה.
3. אם לא מונה בגוף התחבורה עובד ייעודי הנושא בתפקיד ממונה על הגנת הפרטיות, ניתן להטיל את ריכוז היבטי הפרטיות הקיימים בפרויקטים על ועדת היגוי ייעודית, צוות קבוע של ההנהלה הבכירה, וכדומה.

תסקיר – בחינה מוקדמת של ההשפעה על הפרטיות

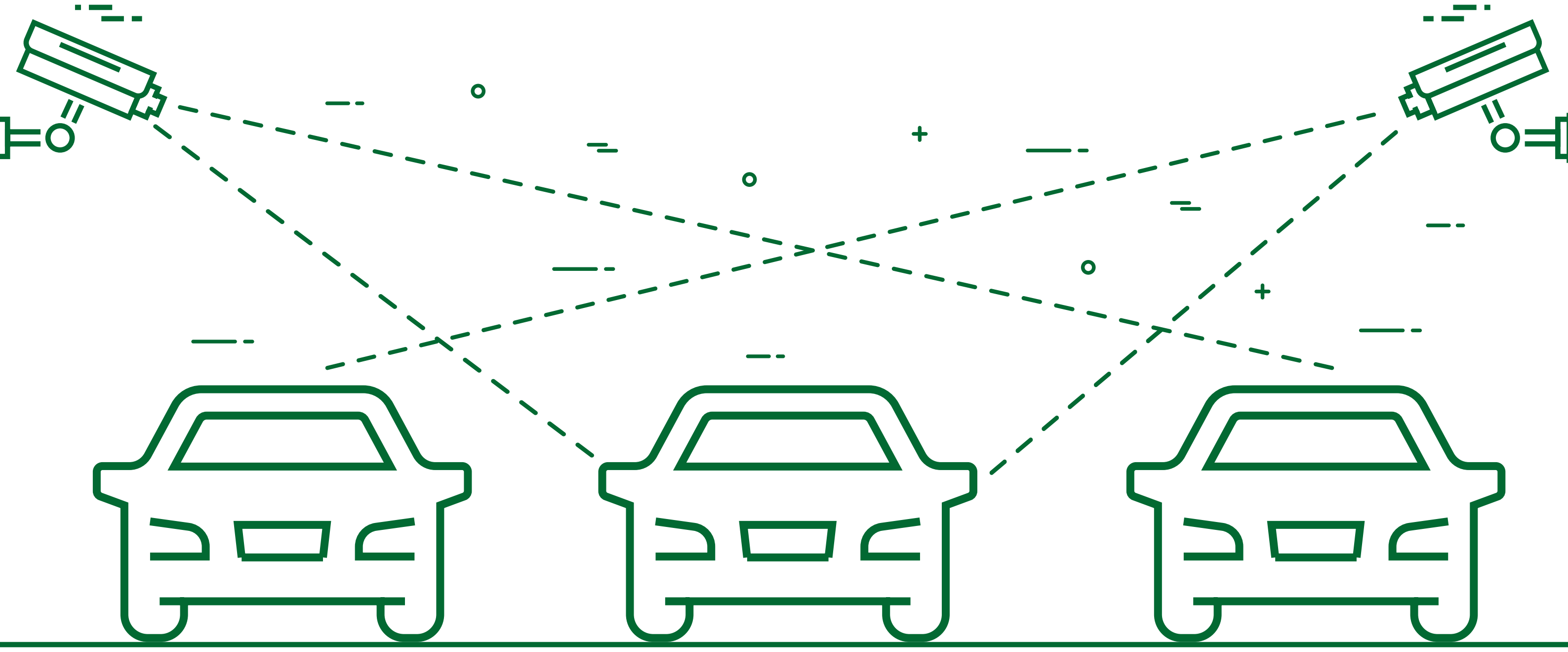
4. הסיכונים הייחודיים והמוגברים לפרטיות המשתמשים אשר עושים שימוש בשירותי תחבורה חכמה באופן שיטתי - מקנים משנה חשיבות להמלצה כי גוף התחבורה יבצע "תסקיר השפעה על פרטיות" (Privacy Impact Assessment) בטרם יספק את השירות. "תסקיר השפעה על פרטיות" הוא הליך מובנה המנתח באופן מקיף ושיטתי את השפעת השימוש בטכנולוגיה על פרטיות נושאי המידע, מזהה את מכלול הסיכונים לפרטיות, בוחן חלופות ומציע את הדרך לצמצם אותם למינימום.
5. עריכה מוקדמת של תסקיר חיונית לבחינת מידתיות השימוש בטכנולוגיות מידע בראי הגנת הפרטיות, ומהווה אמצעי יעיל למימוש החובות שמטיל החוק על בעל מאגר. כמו כן, יצוין כי חלק מרכיבי התסקיר חופפים לדרישות הקיימות בסעיפים 2 ו–5 לתקנות אבטחת מידע המחייבות הכנת 'מסמך הגדרות מאגר' ועריכת מיפוי של המערכות הטכנולוגיות המשמשות את המאגר.

עיצוב לפרטיות

6. המסקנות שיעלו מן התסקיר יתוו את הדרך בה יישם גוף התחבורה את תפיסת 'העיצוב לפרטיות' (Privacy By Design או PBD) וקונספט 'פרטיות כברירת מחדל' (Privacy by Default) (שיכונו להלן ביחד – עיצוב לפרטיות). תפיסות אלו דוגלות בעיצוב מערכת המידע להגנה אופטימאלית על הפרטיות ולצמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם וגם לאורך כל מחזור החיים של איסוף המידע והשימוש בו.

דוגמה

בהקמת כביש אגרה יש לבחור אמצעי לסריקת רכבים ונוסעים על מנת לקבוע חיוב במידה ומספר הנוסעים אינו עולה על הנדרש (נתיב תחבורה ציבורית ושיתופית). בבחינת האלטרנטיבות, הצבת מצלמות יאפשרו זיהוי פנים וזיהוי אישי של הנהג והנוסעים, ואילו במסגרת פתרון המשתמש במצלמות לסריקת חום, תתאפשר ספירה של מספר הנוסעים ללא זיהוי אישי. יש לבחון את האלטרנטיבות ולשלב תכנון לפרטיות בשלב מוקדם.



שקיפות

7. מומלץ כי גוף התחבורה ינהג בשקיפות ויביא לידיעת המשתמשים והציבור את הפרטים המהותיים הנוגעים לשימוש במידע אישי: סוגי המידע הנאסף; השימושים שיעשו בו; האמצעים הננקטים לאבטחת המידע; סיכוני האבטחה; הגורמים אליהם המידע יהיה זמין ולאילו שימושים. כן יש להסביר למשתמשים האם באפשרותם לבחור להימנע מאיסוף המידע, כגון בדרך חלופית לקבלת שירות או שימוש בתשתית שלא כרוכה באיסוף מידע אישי.

8. מומלץ כי המידע שעל גוף התחבורה למסור למשתמש בטרם קבלת מידע ממנו, לפי סעיף 11 לחוק, יפורסם במתכונת נגישה וברורה שתאפשר לתושבים לקבל החלטות מושכלות בדבר אופן השימוש בשירותי גוף התחבורה ומתקניו. רצוי שהמידע הרלבנטי יהיה נגיש הן בסמוך לשירות או לחיישן הנוגע בדבר, והן באופן מרוכז, למשל באזור ייעודי באתר האינטרנט או באפליקציה שלו.

9. השקיפות נדרשת גם לפי הוראות חוק הגנת הפרטיות, וצפויה להגביר את אמון הציבור בגוף התחבורה ובטכנולוגיות בהן הוא משתמש.

שימוש במיקור חוץ ושיתוף פעולה עם גורמים מסחריים

10. במקרים מסוימים המשתמשים בשירותי התחבורה מהווים מעין "קהל שבוי" שאין בידיו האפשרות להימנע משימוש בשירות או בתשתית הכרוכים באיסוף מידע אישי. מסיבה זו, וכן בשל רגישות המידע שניתן להסיק מההיקף הגדול והמגוון של הנתונים הנאספים, נדרש גוף התחבורה להקפדה יתרה בשיתופי פעולה עם גורמים מסחריים נוספים.

11. ראוי שההחלטה בנושא זה תתקבל בדרגים הבכירים ביותר של גוף התחבורה.

12. על מכרזים או חוזים הנערכים בין גוף התחבורה לגורמים מסחריים נוספים בנוגע לפרויקטים הכרוכים בהפעלת טכנולוגיית מידע, לכלול התייחסות מפורטת להיבטי פרטיות ואבטחת מידע, בין השאר בשים לב להנחיית הרשות להגנת הפרטיות בנושא מיקור חוץ לעיבוד מידע אישי, ולהוראות תקנות אבטחת מידע.

פרק 6 | נושאים במיקוד

שאלות מנחות לבדיקה עצמית

בחלק זה מובאות שאלות מנחות לצורך בחינה עצמית של גוף התחבורה, על מנת לסייע לגופי תחבורה ליישם החוקים והתקנות בתחום. מומלץ לקרוא ולבצע בשאלות שימוש לזיהוי אתגרים ומכשולים, בעיקר בשלבים מוקדמים של מיזמים.

המקרים בהם מומלץ על יישום תסקיר השפעה על פרטיות בגוף התחבורה

- מערכת מידע חדשה אשר שומרת או מעבדת מידע אישי.
- פרויקט שיתוף מידע אישי בין ארגונים.
- הצעה לזהות קבוצת אנשים לפי קריטריון משותף על מנת להניע לפעולה.
- שימוש במידע קיים לפרויקט חדש או למטרה חדשה.
- שימוש בנתוני מעקב ובנתוני מיקום.

איסוף ושמירת מידע

- מהם פרטי המידע הנדרשים לצורך מטרת הפרויקט/מיזם?
- לאיזו מטרה נאסף המידע?
- האם מוחזק מידע לא מדויק, חסר או לא מעודכן?
- האם מוחזק מידע עודף, או לא רלוונטי למטרת איסופו/החזקתו?
- במידה שהמידע התקבל ממקור מסוים, האם מצוין מהיכן התקבל? אם המידע לא התקבל ישירות מבעל המידע, האם התקבל כדין ובהתאם להוראות החוק?
- מה משך הזמן ההכרחי לשמור כל סוג מידע? האם המידע מוחזק לזמן רב מדי?
- האם נושא המידע (המשתמש) הסכים להעברת כל המידע אודותיו לארגון לצורך המטרה שהוגדרה?

אבטחת המידע

- האם המידע נשמר במאגר מאובטח העומד בהנחיות המתאימות לסוג המאגר? (הרחבה בפרק 4 ובתקנות אבטחת מידע).
- האם מונה למאגר המידע מנהל מאגר? ממונה אבטחת מידע? האם הוגדרו הרשאות באופן ראוי ואשר תואם את התקנות בחוק?
- האם הגישה למאגר מוגבלת רק לעובדים הכרחיים (בין אם למאגר עצמו או למערכת מידע השולפת נתונים מהמאגר)? כיצד מיושמת הגבלת הגישה?

שימוש במידע

- האם נעשה במידע שימוש שלא למטרה שלשמה הוא נאסף? כיצד מבוצע הפיקוח בעניין זה?
- האם מידע מועבר לצדדים שלישיים? אם כן, האם נושא המידע הסכים באופן מפורש להעברת המידע אודותיו? כיצד מבוצע הפיקוח על העברת המידע?
- האם נעשה שימוש במידע למטרת דיוור ישיר? האם התקבל אישור מנושא המידע להשתמש בפרטיו לצורך דיוור ישיר?
- האם הדיוור הישיר עומד בהוראות החוק?

עיבוד מידע

- האם המידע עובר התממה (הסרת פרטים מזהים כגון שם, ת.ז וכדומה) במידת האפשר?
- האם קיימים מספר מאגרי מידע שונים שבהצלבתם ניתן לזהות את נושא המידע?
- האם מבוצע ניתוח ועיבוד למידע שבמאגר על מנת להסיק תובנות או לזהות דפוסים? במידה שכן, איזה שימוש ייעשה בתוצרי העיבוד שמתקבלים? האם שימוש זה במידע עומד במטרה לשמה נאספו הנתונים מלכתחילה?

זכויות נושא המידע (האדם שמידע אודותיו מוחזק במאגר המידע)

- האם לנושא המידע עומדת האפשרות לעיין במידע אודותיו?
- האם לנושא המידע עומדת האפשרות לתקן פרטי מידע אודותיו?
- האם לנושא המידע עומדת האפשרות לדרוש הפסקת הדיוור הישיר אליו? האם פרטי המידע אודותיו נמחקים ממאגר הדיוור הישיר כתוצאה מבקשה זו?

מדיניות פרטיות

- האם קיימת מדיניות פרטיות לגוף התחבורה?
- האם מדיניות הפרטיות של גוף התחבורה מפורסמת באפיקים המקובלים בהקשר לפעילותו?
- האם קיים תפקיד ממונה הגנת הפרטיות (במשרה מלאה או כנוסף על תפקיד) בגוף התחבורה?
- האם מבוצעות הדרכות או מועברים נהלי פרטיות לעובדים, בדגש על עובדים רלוונטיים (כדוגמת מנהלי מאגרים)?
- האם תחום הפרטיות מוכר על ידי היועצים המשפטיים בגוף התחבורה? האם נבדק באופן תדיר?
- האם מבוצע תהליך ניהול סיכונים בתחום הפרטיות ואבטחת המידע בגוף התחבורה?

כלים לשימוש נכון בנתוני עתק (Big Data)

גופי תחבורה מבצעים איסוף ושימוש בנתונים פרטיים של משתמשים להפעלת שירותי הליבה של פעילותם, וזאת כחלק **מתפיסת ארגון מונחה מידע וקבלת החלטות מבוססת נתונים (Data Driven).** גופים אלו מפעילים שירותים שונים, מתוכם נוצר ידע על ידי פעולות שונות כמו ניתוחים סטטיסטיים של נתונים, אגרגציה של נתונים להפקת תובנות ועוד. בנוסף, ייתכן וגופי תחבורה ירצו להעביר מידע ביניהם, או להקים במשותף **מאגר מידע פתוח (Open Data Source)** שיאפשר צמיחה כלכלית-חברתית או שיתופי פעולה עסקיים.

בעקבות הרצון לבצע ניתוח ועיבוד למידע, לבצע בו שימוש משני ולהעבירו בין גורמים שונים – במקרים בהם הדין מתיר זאת ובהתאם לתנאים הקבועים בדין, עולה בפני גופי התחבורה השאלה – **כיצד ניתן להפוך מידע מזוהה למידע שאינו מזוהה** – קרי מידע שניתן להשתמש בו ולהעבירו תוך צמצום הפגיעה בפרטיות משתמשים? ומה הכלים בהם ניתן להשתמש על מנת לבצע פעולה זו? **תהליך זה נקרא התממה (אנונימיזציה)** – תהליך שמטרתו צמצום הסיכון לזיהוי נושא המידע (המשתמש) או לחשיפה של מידע אישי אודות אנשים שנתוניהם מוחזקים במאגר מידע באופן שעלול להביא לזיהויים.

דוגמה לשלבים בתהליך צמצום הסיכון לזיהוי של נושא המידע

1. **הגדרת שדות של נתונים מזהים ישירים –** שם, ת.ז., מספר מזהה אחר, מספר טלפון וכל נתון חד-חד ערכי אשר מאפשר זיהוי פרטני.
2. **הגדרת שדות נתוני מפתח** שיאפשרו הצלבה של המידע עם מאגר מידע חיצוני ובכך ניתן יהיה לשחזר את הנתונים שהושמטו ולשייך את המאגר לאנשים פרטיים. דוגמה: עיר מגורים, הכנסה, מגדר ועיסוק שבהצלבתם עם משתנים נוספים ניתן יהיה להבין באיזה משתמש מדובר.
3. **הגדרת תרחישי חשיפה והערכת סיכון לקובץ הנתונים –** שלב זה מחולק לשני חלקים. האחד, הערכת סיכונים ותרחישים אפשריים לזיהוי פרטים על ידי מאגר הנתונים המותמם עצמו או על ידי הצלבת הנתונים. השני, בחינת אלטרנטיבות להשמטת ומניפולציה של נתונים ואפשרויות לשחזור הזיהוי.
4. **בחינת שכיחויות –** בחינת מספר הפעמים בהן מופיע נתון מסוים על מנת לבדוק יכולת שחזור. לדוגמה: אם שדה גיל הפך לקבוצות גיל, ובאחת הקבוצות מופיע רק אדם אחד, ניתן יהיה לשחזר מיידית את פרטיו.

5. **כלי התממה לדוגמה:**

א. השמטת שדות זיהוי ישיר ושדות מפתח לזיהוי בהצלבה חיצונית. לדוגמה: החלפת ת.ז. עם שדה מספר סידורי על מנת להבחין בין פרטים שונים במאגר הנתונים.

ב. קידוד נתונים על ידי מניפולציה למשתנים כמותיים דוגמת גיל או הכנסה, המבוצעת באמצעות הרחבת מספר מדויק לטווח. למשל גיל 37 ל "גילאי 30-40" או הכנסה של 12,500 שקלים ל"בין 10,000-15,000".

ג. נתונים סטטיסטיים – ביצוע ניתוח סטטיסטי לשדות אותם מעוניינים להשמיט והעברת פלט (ממוצע, התפלגויות, שונות וכו') לגורם חיצוני על מנת להעביר ידע נצבר ללא פגיעה בנתונים.

ד. כלים נוספים – קיימים מגוון כלים סטטיסטיים נוספים אותם ניתן להפעיל על שדות במטרה לשמור על יעילות המידע תוך הגנה על פרטיות המשתמשים. כלים אלו משנים את הנתונים על ידי הוספת רעשים קבועים או רנדומליים, שמשמרים נתונים סטטיסטיים אגרגטיביים אך משנה את נתוני המשתנה עבור כל פרט.

6. **הערכה של סיכון קובץ הנתונים**, לאחר הפעלת הכלים להתממה. חלק זה מתמקד בבחינת היכולת לשחזר נתונים או ביצוע זיהוי נקודתי של פרטים במאגר.

כלים לשימוש נכון במצלמות

מצלמות לאיסוף מידע ואבטחה

במהלך העשורים האחרונים גובר השימוש באמצעים טכנולוגיים המיועדים לפיקוח ולמעקב חזותי וקולי מרחוק במרחב הציבורי. שימוש זה בא לידי ביטוי בהצבת מצלמות זעירות במקומות רבים במרחב הציבורי. טכנולוגיות אלה, הנקראות (Closed Circuit Television CCTV או Surveillance Video, הן בעלות השפעה מהותית על המרחב הציבורי והשימוש בהן כרוך בפגיעה בפרטיות. מצלמות מעקב משמשות ערים, חברות ונותני שירותים רבים בעולם ובישראל במגוון תחומים – החל ממצלמות אבטחה וביטחון המסוגלות לזהות פנים ולנתח דפוסי תנועה בשירות רשויות ההצלה ואכיפת החוק, דרך מצלמות המנטרות תנועת כלי רכב או ממוקמות על גבי כלי רכב ציבוריים למטרות שונות, ועד מצלמות הממוקמות על עמודי תאורה ציבוריים ומנטרות תנועה למטרות חיסכון באנרגיה ומצלמות לשם פיקוח על חנייה. במרחב ציבורי שכזה, תחושת המעקב התמידי הופכת מוחשית מאי פעם.

השפעת השימוש במצלמות במרחב הציבורי עשויה להיות חיובית, כאשר היא מצמצמת התנהגות עבריינית או מובילה לאופטימיזציה בשירותים הניתנים לציבור. מנגד, ההשפעה עלולה להיות שלילית, כאשר חלק ניכר מהפעילויות הנתפסות באמצעי התיעוד הדיגיטליים הן פעילויות שגרתיות ותמימות, שאינן מהסוג שהחברה (society) בכללותה מבקשת למנוע. בנוסף, ההתפתחויות ביכולת עיבוד הנתונים, דוגמת זיהוי פנים אוטומטי וזיהוי מספר לוחיות רישוי, כמו גם ביכולת ניתוח התוכן המצולם (למשל, ניתוח דפוסי נהיגה או התנהגות במרחב הציבורי), והעובדה כי ישנה תפוצה רחבה של התופעה בערים בכל העולם, מעצימות את פוטנציאל הפגיעה בפרטיות הטמון במצלמות, ומחדדות את תחושת המעקב וניטור פעולות האזרחים.

בשנת 2012 פרסמה הרשות להגנת הפרטיות הנחיה בנושא 'שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן'. הנחייה זו מבהירה את תחולתם של דיני הגנת הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הגנת הפרטיות, שהפרתם עלולה להביא לצעדי אכיפה מנהלית ואף להגיע לכדי עבירה פלילית. בנוסף, פרסם משרד הפנים בשנת 2018 נוהל בנושא שימוש במצלמות לצורך אכיפת עבירות חניה ברשויות המקומיות.

להלן מובאים בצורה מתומצתת, הקווים המנחים והעקרונות המרכזיים עליהם מחויבים גופי התחבורה להקפיד בעת הטמעת טכנולוגיות של פיקוח, ניטור ומעקב חזותי באמצעות מצלמות, וכן בניהול מאגרי המידע והצילומים הנקלטים בהן. הדין המחייב הוא הכתוב בגוף החוק ובהנחיה עצמה.

1. **תכלית הצבת המצלמות ושמירה על עקרון צמידות המטרה והמידתיות –** עוד בטרם הצבת מצלמות ושימוש במערכות ניתוח תמונה, **מומלץ כי הארגון יערוך תסקיר השפעה על פרטיות** (פירוט בדף מידע – שאלות מנחות לבדיקה עצמית). תסקיר הינו הליך המבוצע על ידי הארגון בשלב מוקדם של התכנון, טרם הטמעת הטכנולוגיה המשתמשת במידע אישי, במטרה לזהות את הסיכונים האפשריים לפרטיות ולעצב את המערכות באופן שיצמצם סיכונים אלו מלכתחילה. מדובר בבדיקה מקיפה הבוחנת את השלכות השימוש במצלמות על זכות הציבור לפרטיות, וזאת תוך התייחסות לנושאים הבאים:

- **תכלית הצבת המצלמות – מטרת המצלמות חייבת להיות מוגדרת באופן חד, ספציפי ומפורש.** לדוגמה – "מצלמות ניטור ומעקב תנועה, אשר אוספות מידע ומנתחות אותו בזמן אמת לשם ייעול מערך התנועה העירוני והגדרת מדיניות תחבורתית בעיר". המטרה צריכה להיות בעלת בסיס עובדתי ("ראויה") – כלומר, קשורה לבעיה שפתרונה מצריך הצבת מצלמות. לאחר שנקבעה המטרה, חל איסור להשתמש בצילומים למטרות זרות, אין להעבירם לגורמים זרים ואין לשמור אותם לאחר שאינם נחוצים עוד.
- **מידתיות לאור המטרה –** הזכות לפרטיות היא זכות חוקתית מוגנת, ולכן עצם קבלת ההחלטה על **שימוש במצלמה בידי גוף תחבורה שהוא רשות ציבורית מחייבת עמידה במבחן המידתיות.** בהקשר זה יש לשאול: האם מצלמות הן האמצעי המתאים ביותר לאור המטרה? האם המטרה מחייבת הקלטה של הצילומים או שניתן להסתפק בצילום חי? (ככל שיש צורך להקליט, יש להגדיר את משך התקופה בה ישמרו הקלטות) האם התועלת למשתמש עולה על העלות (במונחי הפרטיות)? האם ניתן להשיג את המטרה באמצעים פחות פוגעניים? אמצעים נוספים למזעור פגיעה בפרטיות ודגשים בנושא שמירת הצילומים ומחיקתם ניתן למצוא בהנחיה המלאה.
- **דגשים נוספים –** כאשר מדובר במצלמות שמוצבות במרחב הציבורי, יש לנקוט משנה זהירות כשמדובר במצלמות המנטרות אוכלוסיות מוחלשות כמו קטינים או קשישים (קירבה למוסדות חינוך או סיעוד וכד'). החלטה מסוג זה תתקבל על ידי הרשויות הממונות (רשות מקומית למשל) ויש לבחון את השפעות הפרטיות בהתאם. **בנוסף, יש להיזהר זהירות יתרה בהקלטה קולית.** על מעקב קולי, הנתפס כרגיש וחודרני, חלות חובות והוראות סדורות כמפורט בחוק האזנת סתר, התשל"ט-1917.

2. **'עיצוב לפרטיות'** (Privacy by Design) – בעת פיתוח שירותים ומוצרים המשלבים מצלמות, **רצוי להקפיד על 'עיצוב לפרטיות', כבר משלב התכנון, ולוודא כי מספר פרמטרים עומדים במבחן הרלוונטיות למטרה ולתכליתן של הצבת המצלמות.** למשל: מיקום וזווית המצלמות – כך שלא יאספו יותר מידע מהמינימום הנדרש (לדוגמה: מצלמת רכב שלא תצלם לתוך בתי עסק ובניינים); **מספר המצלמות –** לא יותר מהמינימום הנדרש; **זמני צילום –** למשל, אם מדובר במצלמות לניתוח תנועה וניתובה, הן עשויות להיות מופעלות בשעות עומסי התנועה

בלבד; **רזולוציה** – למשל, אם המטרה היא מערכת לניתוב תנועת כלי רכב, אזי קיים צורך לזהות לוחיות רישוי, ולכן יש צורך בצילום ברזולוציה גבוהה. מנגד, תאורה חכמה שנועד לחסון בצריכת אנרגיה אינו מחייב צילום ברזולוציה גבוהה שיכולה לזהות פנים.

3. **זכות העיון – כפי שהוזכר, מחובת נותן השירות לאפשר לאנשים שעליהם נאסף מידע לעיין במידע זה**, זאת תחת תנאים ספציפיים המוסדרים בסעיף 13 לחוק ובתקנות הגנת הפרטיות (תנאים לעיין במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981. הקלטות המצלמות מהוות גם הן מאגר מידע עליו חלה זכות העיון, אולם במימוש זכות העיון במאגר הצילומים **ישנם דגשים פרקטיים ומשפטיים עליהם יש לתת את הדעת, בעיקר כדי למנוע פגיעה בפרטיות צדדים שלישיים העשויים להופיע בצילום.** הרחבה בסעיף 3.1.5 להנחיה המלאה.

4. **אבטחת המידע הנאסף** – בהמשך לאמור בחלקים הקודמים, המנגישים את נושא ניהול המאגרים ואבטחתם, סעיף 17 לחוק הגנת הפרטיות מטיל על בעל המאגר, מנהלו והמחזיק בו את האחריות לאבטחת המידע המצוי במאגר. בתוך כך, **מחובת הארגון לוודא קיום הגנה פיזית ולוגית על מערכת מצלמות המעקב, להגדיר נהלים ברורים להקלטת הצילומים,** לעיבודם ולהפצתם ולאבטחת המידע בהם, ולקבוע **רשימה מוגבלת של מורשי גישה למידע.** כמו כן, באחריות הארגון **לנקוט במשנה זהירות בעת העזרות בגורמים חיצוניים.** מידע נוסף ניתן למצוא באתר הרשות להגנת הפרטיות ובמדריך המלא ליישום תקנות אבטחת מידע.

תחבורה במרחב העירוני

מגמת נוכחות הרשויות המקומיות בחיי התושבים הולכת וגוברת. ההשפעה של הרשות המקומית על התושב בעידן הדיגיטלי מתחזקת ואחת ההשלכות המרכזיות היא בתחום התחבורה. רשויות מקומיות רבות מבינות כי סוגיית התחבורה במרחב העירוני היא אחת מנקודת "התורפה" בהן נדרש טיפול רחב ומידי ומציאת פתרונות יצירתיים ודיגיטליים. מענה טוב לבעיות התחבורה באזור מיושב יאפשר שיפור שירות, התייעלות כלכלית וניצול נכון של משאבים.

התחבורה בעידן הדיגיטלי מתפתחת במהירות על ידי ענקיות טכנולוגיה בינלאומיות ועל ידי חברות הזנק מקומיות כאחד, וזאת בשאיפה להקל ולשפר את איכות החיים והתנועה בעיר, תוך מקסום הבטיחות של התושבים, הנהגים והנוסעים.

תחום התחבורה מהווה אחד מעמודי התווך של העיר החכמה. תחום זה כולל, בין היתר, נסיעות משותפות, תחבורה ציבורית, ניטור ובקרת תנועה, חניה, אכיפה ותשלום ועוד.

על מנת להפעיל מיזם תחבורתי נדרש שימוש בנתונים שונים, ובמקרה של מיזם תחבורתי בערים חכמות שימוש בנתונים הכוללים מידע אישי של תושבים ושל אנשים הנעים במרחב המיושב. לצד המטרות החיוביות של הכנסת פרויקטים אלו לרשות המקומית, מיזמים תחבורתיים שונים עושים שימוש בחיישנים המצלמים וסורקים מכשירי מדיה דיגיטלית, רכבים ותושבים, או אפליקציות הקוראות נתונים אישיים מתוך המכשיר הפרטי של המשתמש, תוך סיכון פוטנציאלי לפגיעה בפרטיות המשתמש.

המידע המובא בפרק זה נועד לסייע לגוף התחבורה ולרשות המקומית בהטמעת מיזם תחבורתי חדש ובהפעלת מיזם תחבורתי קיים, ומכיל המלצות לבדיקת הרבדים והמרכיבים השונים במטרה למנוע פגיעה בפרטיות התושבים.

פרק זה מגדיר את האופן שבו רואה הרשות להגנת הפרטיות את תכולת תחום התחבורה בעיר החכמה, מנתח את הסיכונים האפשריים לפרטיות, ומנחה כיצד יש לנהוג בתכנון והקמה של מיזם תחבורתי ובעת הפעלת מיזם תחבורתי.

תחבורה במרחב העירוני בראייה כוללת

תחום התחבורה בעיר החכמה עשוי להכיל מאות רבות של מיזמים מסוגים שונים, המתבססים על אמצעים טכנולוגיים רבים – החל מפריסת מצלמות ועד אפליקציות עירוניות. ניתוח שערכה הרשות במסגרת כתיבת המדריך העלה שישה תתי תחומים עיקריים ומשמעותיים בתחום התחבורה בעיר החכמה לגביהם נערך ניתוח של הסיכון לפגיעה בפרטיות התושבים.

תחום התחבורה החכמה הינו תחום דינמי ומתפתח. הטבלה הבאה מתארת טכנולוגיות קיימות ועתידיות נכון לרגע כתיבת המדריך והיא נועדה לסייע לגופי התחבורה ולגורמים רלוונטיים אחרים, לערוך ניתוח של מיזם קיים או עתידי בראי הסיכונים לפרטיות תושבים.

תחום	תת תחום	פירוט	רמת הסיכון לפגיעה בפרטיות
נסיעות משותפות	שיתוף נסיעות	שיתוף נסיעות ברכבים פרטיים אישיים (Carpooling). משתמשים נרשמים לשירות שמאפשר להם לצרף נוסעים לנסיעה או להצטרף לנהגים אחרים בעבור תשלום. מעקב אחר מספר הנוסעים נעשה, בין היתר, באמצעות טכנולוגיות לספירת נוסעים ברכב.	סיכון גבוה לפרטיות – שמירת פרטי משתמשים, פרטי תשלום ומסלולי תנועה, חיבור למכשיר סלולרי.
	שיתוף כלי רכב	כלי רכב שיתופיים בבעלות ספקים חיצונים: רכבים, אופניים וקורקינטים. הספק, לאחר הסכם עם הרשות שבשטחה תפעל, מפזר כלי רכב בעיר ומאפשר למשתמשים לשכור את כלי הרכב לפרקי זמן קצרים.	סיכון גבוה לפרטיות – שמירת פרטי משתמשים בידי ספק חיצוני, פרטי תשלום ומסלולי תנועה, חיבור למכשיר סלולרי.
	רכבים אוטונומיים שיתופיים	רכב שיתופי אוטונומי – מונית חכמה. שירות מוניות אוטונומיות זהה לשירות מוניות רגיל.	סיכון גבוה לפרטיות – שמירת פרטי משתמשים, פרטי תשלום ומסלולי תנועה, חיבור למכשיר סלולרי.
תחבורה ציבורית	שירות מוניות חכם	שירות הזמנת מוניות, בקרת נסיעה ותשלום דיגיטלי דרך אפליקציה מבוססת מקום.	סיכון גבוה לפרטיות – זיהוי משתמש, פרטי אשראי, שמירת מיקום.
	תחנות תח"צ חכמות	תחנות תחבורה ציבורית חכמות המאפשרות הצגה ודחיפה של מידע למשתמש לגבי זמני הגעה והודעות נוספות. מלווים במסכים, מערכת כריזה או אמצעי דחיפה למכשירי המשתמשים. מחוברים למערכת מבוססת GPS בכלי התחבורה (אוטובוס או רכבת) לבקרת מיקום בזמן אמת.	סיכון תלוי בסוג התחנה. אם מוצבות מצלמות או חיישן המתקשרים עם מכשירים סלולריים קיים סיכון גבוה לפרטיות.
	מידע תח"צ בזמן אמת	העברת מידע לגבי תחבורה ציבורית בזמן אמת למשתמשים על ידי תחנות (כפי שהוצג בסעיף תחנות חכמות) או על ידי שירות חיצוני המאפשר גישה לאפליקציה המציגה מידע בזמן אמת לגבי תנועת כלי רכב ציבוריים (אוטובוסים, מוניות שירות ורכבות)	במידה והמידע מבוסס על חיישני GPS באוטובוס והצגת מידע לגבי תנועת תח"צ בלבד, דוגמת זמני הגעת האוטובוס, אין סיכון משמעותי לפרטיות.
	כרטיסי נסיעה חכמים רב ערוצים	כרטיס תשלום משולב למספר ערוצים – אוטובוסים, רכבות ושירותי תחבורה ציבורית נוספים.	סיכון תלוי במאגר המידע. אם קיים מאגר מידע בו נשמרות רשומות נסיעה – סיכון גבוה לפרטיות. אם מבוצע תשלום בלבד באמצעות הכרטיס באמצעים המקובלים ללא שמירת נתונים – סיכון פחות לפרטיות.
	אפליקציות ארנק וירטואלי כרטיסי נסיעה	מערכת מתקדמת לכרטיס הנסיעה החכם. אפליקציית ארנק לתשלום דיגיטלי, ממשק עם מערכות בקווי תחבורה ותשלום ישיר.	סיכון גבוה יותר מכרטיס תשלום פיזי. קישוריות למכשיר סלולרי מעלה רמת סיכון.
	אוטובוס חכם	שירות המאפשר התאמת מסלול בזמן אמת בהתאם לדרישת משתמשים באפליקציה. מסלול כלי הרכב נקבע לפי אזור מוגדר ולא נתיב קבוע לפי רחובות וההתאמה נעשית בזמן אמת.	סיכון גבוה לפרטיות – שמירת פרטי משתמשים, פרטי תשלום ומסלולי תנועה, חיבור למכשיר סוללרי

תחום	תת תחום	פירוט	רמת הסיכון לפגיעה בפרטיות
ניטור ובקרת תנועה	ניטור ומעקב תנועה בזמן אמת	שירות משלים למעקב התנועה. מערכת שליטה על רמזורים המאפשרת אופטימיזציה של התנועה ברשות וניתוב כלי רכב לפי עומסים.	סיכון תלוי במאפייני רשת המצלמות – סיכון גבוה ברזולוציה גבוהה ויכולת זיהוי פרטי רכב וזיהוי פנים. סיכון נמוך אם מבוצע זיהוי עומס תנועה בלבד.
	מערכות בקרת רמזורים ואופטימיזצית תנועה	כלי רכב שיתופיים בבעלות ספקים חיצונים: רכבים, אופניים וקורקינטים. הספק, לאחר הסכם עם הרשות שבשטחה תפעל, מפזר כלי רכב בעיר ומאפשר למשתמשים לשכור את כלי הרכב לפרקי זמן קצרים.	סיכון גבוה לפרטיות – שמירת פרטי משתמשים בידי ספק חיצוני, פרטי תשלום ומסלולי תנועה, חיבור למכשיר סלולרי.
	רמזור חכם למניעת תאונות	מערכת המתממשקת לרשת הרמזורים תוך שילוב מצלמות וחיישני תנועה שמטרתה להתריע בפני סכנות ולשלוט בתנועה במידת הצורך על מנת למנוע תאונות.	סיכון תלוי במאפייני רשת המצלמות – סיכון גבוה ברזולוציה גבוהה ויכולת זיהוי פרטי רכב וזיהוי פנים. סיכון נמוך אם מבוצע זיהוי עומס תנועה בלבד.
חניה	תשלום חניה	תשלום חניה דרך שירות באפליקציה. שימוש בחניה עירונית (כחול-לבן) ובחניונים.	סיכון גבוה
	חניה חכמה	רשתות שיתופיות למקומות חניה. מערכת ייעודית או כזו הנשענת על רשת קיימת (קבוצות או רשתות חברתיות) המאפשרת שיתוף בנוגע למקומות חניה פנויים ברשות והכוונה אליהם.	סיכון תלוי בסוג החיישן –אם מבוסס מצלמות ושמירת מאגר הצילום, סיכון גבוה לפרטיות. אם מבוסס חיישן תנועה – אין סיכון לפרטיות.
	חניה שיתופית	העברת מידע לגבי תחבורה ציבורית בזמן אמת למשתמשים על ידי תחנות (כפי שהוצג בסעיף תחנות חכמות) או על ידי שירות חיצוני המאפשר גישה לאפליקציה המציגה מידע בזמן אמת לגבי תנועת כלי רכב ציבוריים (אוטובוסים, מוניות שירות ורכבות)	סיכון בינוני – גבוה לפרטיות – שימוש במכשירים סלולריים. אם מבוצע שימוש במאגר מידע השומר רשומות – סיכון גבוה יותר.
אכיפה ותשלום	מצלמות אכיפה	מערכת אכיפה באמצעות מצלמות ושליחת דוחות וקנסות אוטומטיים. בשימוש לנתיבי תחבורה ציבורית, נתיבים לרכב רב-תפוסה, שבילי אופניים, חניה, צמתים ותמרורים.	סיכון גבוה מאוד לפרטיות – זיהוי פרטני וחיבור למאגר מידע עם פרטים אישיים.
	כבישי אגרה	מערכת מבוססת מצלמות וחיישנים לזיהוי וחיוב כלי רכב. כבישי אגרה מוגדרים ואגרות גודש במרכזי ערים.	סיכון גבוה מאוד לפרטיות – זיהוי פרטני וחיבור למאגר מידע עם פרטים אישיים.
אחרים	מתן מידע בהתאמה אישית ובדחיפה באמצעות ,BT) RF וכו')	מערכות דחיפת מידע למכשיר המשתמש על יד מסרון או הודעות דחיפה (Push Notification). מבוססות מקום – שולח למשתמשים באזור מוגדר, או רישום לשירות ומאפשר שליחה לפי חיתוכי קבוצות משתמשים.	סיכון בינוני לפרטיות – איתור מכשיר סלולרי לפי פרטים ומיקום. סיכון גבוה לפרטיות – אם מותקנת אפליקציה על המכשיר לקבלת המידע.
	טעינת רכבים חשמליים	ממשקי טעינת רכבים חשמליים בחניונים ציבוריים בתשלום מקומי או דיגיטלי.	אם מבוצע תשלום ללא שם משתמש וזיהוי פרטים, סיכון נמוך מאוד לפרטיות.

דוגמה

רמזור חכם למניעת תאונות

רשות מקומית מעוניינת בהקמת רשת רמזורים חכמים שתסייע במניעת תאונות. בכל צומת מרכזי תחובר רשת של מצלמות למערכת שמנטרת תנועה בזמן אמת ומקושרת לרמזורים על מנת לנתב תנועה במידת הצורך. לצורך הדוגמה, נצא מנקודת הנחה כי המערכת אוספת מידע כהגדרתו בחוק הגנת הפרטיות. המערכת ושירותי הפעלתה יסופקו על ידי חברה חיצונית שתיבחר במכרז של הרשות המקומית.

תכנון והקמה:

טרם הקמת המיזם, יבוצע תסקיר **השפעה על פרטיות** (באתר הרשות להגנת הפרטיות ניתן למצוא כלי עזר לביצוע התסקיר) על מנת לזהות סיכונים וגורמים היכולים להוות פגיעה בפרטיות האזרחים. התסקיר יסייע לבחור **באלטרנטיבה הפוגעת באופן המינימלי ביותר בפרטיות** מבין האפשריות השונות להקמת המיזם. **עיצוב לפרטיות** יבוצע טרם הקמת הפרויקט. מוביל הפרויקט יוודא תיעוד תהליכי קבלת החלטות בפרוטוקולים לקראת פרסום לציבור במטרה לייצר שקיפות בנוגע למיזם ולרשת המצלמות שתוצב.

הרשות המקומית תרשום את המאגר אצל רשם מאגרי המידע ברשות להגנת הפרטיות. בקשת הרישום תפרט, בין השאר, את זהות בעל המאגר, המחזיק במאגר ומנהל המאגר; מטרות הקמת המאגר, סוגי המידע שייכללו במאגר ועוד.

כחלק מהחובה לעמוד בהוראות תקנות אבטחת מידע, הרשות המקומית תגדיר הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר. בהתאם להגדרות התפקיד הרשאת הגישה לכל בעל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

באשר לשימוש במיקור חוץ, כאשר הרשות המקומית עורכת מכרז או חוזה עם גורם חיצוני בנוגע לפרויקט הכרוך בהפעלת טכנולוגיית מידע, מחובתה לכלול התייחסות מפורטת להיבטי פרטיות ואבטחה, בין השאר בשים לב להנחיית הרשות להגנת הפרטיות בנושא שימוש במיקור חוץ לעיבוד מידע אישי ולהוראות תקנות אבטחת מידע.

הפעלה ומימוש:

על מנת **לצמצם פגיעה בפרטיות** תושבים או עוברי אורח אשר עשויים להיות מצולמים, מוצע כי מצלמות המיועדות לניתוח תנועת כלי רכב, יופנו לכביש וכלל לא יצלמו את המדרכות, לרבות צילום מעברי חציה, ולא יתעדו כניסות לבתים ובתי עסק. מעבר לכך, איכות התמונה תהיה ברזולוציה נמוכה על מנת שלא תוכל לאפשר זיהוי פנים, אך חדה מספיק בכדי להבחין בתנועת רכבים והולכי רגל. ככל שהמצלמות מיועדות לנתח את תנועת הולכי הרגל, לדוגמה לשם הגברת בטיחותם, ייתכן ויהיה מקום לצילום אזורי המדרכות, אך גם כאן יש לדאוג כי רזולוציית הצילום לא תאפשר זיהוי פנים.

מערכת המידע תשמור את הנתונים במשך 24 שעות על מנת שיהיה ניתן להוציא ממנה בזמן אמת קטעים עבור תחקור ובדיקת מידע. לאחר מכן המידע ימחק בכפוף לחריגים הקבועים בחוק. מטרת השימוש במידע תוגדר לצורך מניעת תאונות, ולכן, מכוח עקרון צמידות המטרה, **לא יעשה שימוש בחומר** המצולם למטרות אכיפה והטלת קנסות, או על מנת לאתר רכב או אדם מסוים, אלא מכוח הסמכה מפורשת בחוק.

מאגר המידע של המערכת יהיה נפרד ממאגרים אחרים ברשות המקומית, והגישה אליו תוגבל רק לבעלי הרשאות גישה. לא ניתן יהיה להעביר את הנתונים או לעשות בהם שימוש בהם למטרה שונה מזו שהוגדרה בהליך עיצוב לפרטיות ובמסמך הגדרת המאגר, אלא מכוח חוק.

מדיניות פרטיות ביישומונים (אפליקציות) לתשלום ולתיקוף בשירותי תחבורה ציבורית

בשנים האחרונות, וכחלק מהשימוש ההולך וגובר בטכנולוגיות מידע לקידום היבטים של "תחבורה חכמה" בארץ ובעולם, אנו עדים להתפתחות השימוש ביישומונים (אפליקציות) לתשלום ולתיקוף השימוש באמצעי תחבורה ציבורית כגון אוטובוסים, רכבת ורכבת קלה.

ככלל, השימוש בטכנולוגיות מידע לקידום היבטים של תחבורה חכמה בכלל, ובמסגרת שימוש בתחבורה ציבורית בפרט, הוא מבורך. שימוש זה עשוי להביא לשיפור יעילות השימוש באמצעי התחבורה הציבורית ואף להוזלת העלויות הכרוכות בו.

עם זאת, שימוש שכזה עלול גם להיות כרוך בפגיעה קשה בפרטיותם של משתמשי התחבורה הציבורית, שחלק ניכר מהם הם למעשה "קהל שבוי" שאין בידיו האפשרות שלא להשתמש בשירותים אלו. תחבורה ציבורית הינה שירות ציבורי חיוני, המבטא את חובתה של המדינה לאפשר לאזרחיה לממש את חופש התנועה שלהם במרחב הציבורי. לאור האמור, ובהינתן ששימוש ביישומונים בהקשר הנדון כרוך באיסוף ועיבוד מידע אישי רב ורגיש, עמדת הרשות להגנת הפרטיות היא כי השימוש ביישומונים אלו צריך להיעשות תוך מתן התייחסות מעמיקה להיבטים של הגנה על פרטיות וכן הגנה על המידע האישי שנאסף, והכל כפי שיפורט בהמשך.

לגישת הרשות, עצם השימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית אינו פסול שלעצמו. עם זאת, שימוש זה צריך להיעשות בצורה סבירה, שקופה והמאזנת כראוי בין הצורך להשתמש במידע על אודות משתמשים לבין ההגנה על פרטיותם. כפי שיפורט בהמשך, דגש מיוחד יש לשים בהקשר זה על סוגיית ההסכמה ועל מתן חלופה אנונימית לשימוש בשירותי תחבורה ציבורית, אם במסגרת היישומונים, ואם במסגרת חלופית אחרת.

יישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית – רקע כללי

באופן מסורתי, התשלום בעבור שימוש באמצעי תחבורה ציבורית נעשה במסגרת שימוש בכרטיסי נייר. בשנים האחרונות, מטעמים של יעילות, נוחות וחסכון, מתרחש מעבר לשימוש באמצעים דיגיטליים לתשלום ולתיקוף השימוש באמצעי תחבורה. אמצעים אלו מוגדרים, בין היתר, כמערכות תחבורה חכמות (ITS – Intelligent Transportation Systems), מערכות כרטוס אוטומטי משולבות לתחבורה ציבורית (integrated e-ticketing systems for public transport), ושירותי תחבורה ציבורית מבוססת חשבון מרוחק (תמ"ר).

האמצעים הדיגיטליים בהם ניתן לעשות שימוש לתשלום ולתיקוף שימוש בתחבורה ציבורית הם מגוונים. אמצעי מרכזי אחד הוא כרטיס אלקטרוני חכם הפועל בטכנולוגיית Calypso, והניתן לטעינה רב פעמית. זהו האמצעי בו נעשה שימוש בישראל בשנים האחרונות ("רב-קו"). אמצעי מרכזי אחר הוא יישומון (אפליקציה) המותקן בטלפון החכם של משתמשי התחבורה

הציבורית, ואשר במסגרתו יכול המשתמש לשלם בעבור שימושו באמצעי התחבורה הציבורית השונים. התשלום יכול להתבצע, בין היתר, באמצעות סריקת קוד QR (Quick Response Code) או באמצעות קירוב מכשיר הטלפון לסורק (טכנולוגיית NFC – Near Files Communication). במקרים מסוימים תיקוף הכרטיס יכול להיעשות גם במסגרת איכון מיקום המשתמש וזאת באמצעות שימוש בטכנולוגייתGPS או טכנולוגיית RFID. אפשרות נוספת היא תשלום על שימוש בשירותי תחבורה ציבורית ישירות באמצעות כרטיסי אשראי. בניגוד לאופן התשלום בכרטיסים חכמים, הנעשה לרוב מראש וללא התייחסות לאופן השימוש בתחבורה הציבורית, יישומונים מאפשרים למשתמשים לשלם בהתאם להרגלי השימוש שלהם, ועל-פי תמחור משתנה. ככלל, המעבר לשימוש באמצעים דיגיטליים לתשלום ולתיקוף שימוש בתחבורה ציבורית הוא חלק מתפיסה כוללת של קידום תחבורה חכמה בישראל ובעולם.

התחבורה הציבורית כשירות ציבורי חיוני

תחבורה ציבורית הינה **שירות ציבורי חיוני. שירות זה מבטא את חובתה של המדינה לאפשר לאזרחיה לממש את חופש התנועה שלהם במרחב הציבורי.** מלבד היותה אמצעי למימוש חופש התנועה, לתחבורה הציבורית יש תפקיד חברתי משמעותי. שכן, עבור אוכלוסיות נרחבות בציבור (כגון ילדים, קשישים, אנשים עם מוגבלות, וכן אוכלוסיות מוחלשות שאין בבעלותן רכב פרטי) התחבורה הציבורית היא האמצעי היחיד המאפשר להן להתנייד במרחב הציבורי, ובכך לממש זכויות אחרות העומדות להן. לתחבורה הציבורית חשיבות גם מבחינה כלכלית ומבחינות נוספות כגון איכות החיים של אזרחי ישראל.

ככלל, על גופים המספקים שירותים ציבוריים חיוניים מוטלות חובות מסוימות הנגזרות מחיוניות השרות, כגון חובת מתן שירות לכל הפונים אליהם (אלא אם יש טעם סביר להימנע מכך), באמצעים סבירים, בתמורה סבירה וללא הפלייה.[2] לאור חשיבותה של התחבורה הציבורית, במשך השנים הושם דגש על היכולת של הציבור להשתמש בתחבורה הציבורית באופן שוויוני. כך לדוגמה, סעיף 19(א) לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998, קובע מפורשות כי אנשים עם מוגבלות זכאים לשירותי תחבורה ציבורית נגישים ומתאימים לשימושם. בית המשפט העליון קבע בהקשר אחר כי הפרדה בין נשים לגברים במסגרת שימוש באוטובוסים המיועדים לחברה החרדית, היא אפליה פסולה.[3]

כל האמור מבטא את חשיבותה של התחבורה הציבורית בישראל וכן את הצורך בהקפדה כי אופן הפעלתה ייעשה בצורה סבירה המכבדת את זכויותיהם של המשתמשים בשירות זה, וזאת ללא רלוונטיות לזהות הגורם המספק את השירות. **מסקנה עקרונית זו צריכה לעמוד ברקע הדברים גם בדיון בדבר הזכות לפרטיות של משתמשי התחבורה הציבורית בישראל.**

2 תא (ת"א) 32053007-17 א.י. איור בע"מ נ' ישרכארט בע"מ (פורסם בנבו, 5.5.2020).

3 בג"ץ 746/07 נעמי רגן נ' משרד התחבורה, סד(2) 530 (2011).

יישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית – אתגרי פרטיות

ככלל, השימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית הוא לגיטימי ואין בו, שלעצמו, בכדי להוות פגיעה בפרטיות. עם זאת, שימוש זה צריך להיעשות תוך מתן התייחסות מעמיקה להיבטי פרטיות ואבטחת מידע, ותוך שימת דגש על סוגיית ההסכמה. התייחסות זו רצוי שתעשה כבר בשלב התכנון הטכנולוגי וטרם השימוש ביישומונים.

השימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית מעלה מספר סוגיות הנוגעות לפרטיות ולאבטחת מידע. להלן יפורטו אתגרי הפרטיות המרכזיים הרלוונטיים לעניין זה:

- **ספק במודעות להסכמה לאיסוף מידע –** על פי חוק הגנת הפרטיות, הסכמה לוויתור על פרטיות צריכה להיות "מדעת". משמעות הדבר היא שבמסגרת בקשת ההסכמה יש להעניק לפרט את כל המידע הרלוונטי עבורו (לרבות מטרת איסוף המידע והשלכות האיסוף), לאורו הוא יוכל לבחון את הבקשה.

עם זאת, מחקרים רבים מעידים כי הליך מתן ההסכמה תוך שלפרט ניתנת האפשרות לעיין בתנאי השימוש, אינו משיג את מטרתו לאפשר לפרט לשלוט על אופן השימוש במידע הנוגע אליו. זאת בין היתר כיוון שמצופה ממנו לקרוא מסמכי מדיניות ארוכים בעת הפעלת היישומון לצורך ביצוע פעולה פשוטה, וכן ולנוכח המורכבות הקיימת בהבנת אופן השימוש במידע דיגיטלי.

דבר זה נכון, בחזקת קל וחומר, כאשר מדובר במתן הסכמה לשימוש ביישומונים בכלל, וביישומונים לתחבורה ציבורית בפרט. במסגרת הליך קבלת הסכמה לשימוש ביישומונים מתבקשים אנשים להעניק הסכמתם לכל האמור במסמכי מדיניות ארוכים, המנוסחים בצורה משפטית ומורכבת. הליך זה מתקיים, לרוב, במסגרת שימושו של האדם בטלפון החכם שברשותו, שהתצורה הטכנולוגית והפיזית שלו לא מתאימה תמיד לקריאת מסמכים ארוכים ומורכבים. מטבע הדברים, במצב שכזה עומד בפני כל אדם קושי אמיתי להבין את משמעות ההסכמה הניתנת על-ידו. מצב זה הינו בעייתי אף יותר בכל הנוגע ליישומונים לשימוש בתחבורה ציבורית, כגון במקרים בהם אנשים יורידו את היישומון זמן קצר לפני שימושם בפועל בשירותי התחבורה הציבורית, מבלי שיש להם פניות לבחון לעומק את הבקשה ואת השלכותיה.

כל האמור מבטא את הקושי בקבלת הסכמה מדעת בהקשר האמור. בעניין זה יש לציין גם כי חלק לא מבוטל ממשתמשי שירותי התחבורה הציבורית הם קטינים עד גיל 18, אוכלוסייה מבוגרת וכן אנשים עם מוגבלות. קהל זה הינו, מעצם מהותו, "קהל שבוי" שבמקרים רבים נעדר יכולת להתנייד במרחב הציבורי ללא שירותי תחבורה ציבורית. מטבע הדברים, קבלת הסכמה לוויתור על פרטיות בקרב אוכלוסיות אלו עשויה להיות בעייתית ולא לעמוד בדרישות הדין בכל הנוגע לקבלת הסכמה מדעת.

- **העדר חלופות – הסכמה חופשית ומדעת של אדם לבקשה לשימוש במידע על אודותיו יכולה להיחשב ככזו רק כאשר עומדת לאדם האפשרות הסבירה לסרב לה.** בהמשך לנקודה שצוינה קודם לכן, אחד החששות המרכזיים בכל הנוגע לשימוש ביישומונים לתחבורה ציבורית (או לשירותים ציבוריים אחרים לצורך העניין), הוא כי אנשים יאלצו לתת הסכמתם לשימוש במידע הנוגע אליהם, וזאת לא מתוך רצון חופשי אלא מחוסר ברירה. מצב זה עלול להיווצר בנסיבות בהן לא תעמוד לאנשים האפשרות המעשית להשתמש בשירותי התחבורה הציבורית, אלא בכפוף לתשלום באמצעות יישומונים אלו. נכון להיום, קיימת בפני ציבור משתמשי התחבורה הציבורית האפשרות להשתמש בכרטיס חכם אנונימי, אשר מאפשר להם לנוע במרחב הציבורי באופן בלתי מזוהה, ותוך שמירה על פרטיותם. אלא שצמצום מספר עמדות הטעינה של כרטיסים חכמים אנונימיים, ומשבוטלה לאחרונה, עבור מרבית האוכלוסייה, האפשרות לשלם באמצעות כרטיסי נייר, ייצור מצב בו הציבור יחויב, דה-פקטו, בשימוש ביישומונים שהשימוש בהם כרוך במתן פרטים מזהים – ויהווה פגיעה קשה בפרטיות, ללא חלופה בת-קיימא לשימוש בתחבורה ציבורית.

- **תחושת מעקב ופגיעה בשליטה במידע** – שימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית, ובמיוחד כזה הנעשה באופן המחייב דה-פקטו שימוש ביישומונים אלו, עלול להיתפס כפגיעה בפרטיות גם בהיבט של תחושת מעקב. מצב זה עלול להביא ליצירת תחושה של מעקב תמידי אחר מיקומו של היחיד במרחב הציבורי, באופן אשר יצטייר כפגיעה בפרטיותו וביכולתו להתנהל במרחב הציבורי באופן אנונימי ובלתי מזוהה. בעניין זה חשוב לזכור כי המידע הנאסף במסגרת שימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית הוא מידע רגיש הכולל פרטים מזהים, ואשר מתוכו ניתן גם ללמוד רבות על פרטי נסיעותיו, שיש בהם כדי ללמד על התנהלותו של אדם ועל אורחות חייו. במצב שכזה, תחושת המעקב והפגיעה בשליטה במידע עלולות להתעצם, ולהיתפס כפגיעה קשה וחמורה בפרטיות.

- **זליגת מידע** – שימוש ביישומונים לתשלום ולתיקוף שימוש בשירותי התחבורה הציבורית כרוך, על-פניו, באיסוף ובעיבוד מידע אישי רב ורגיש על אודות משתמשים בתחבורה ציבורית כגון פרטים מזהים (שם פרטי ומשפחה, מספר ת.ז), גיל, פרטי התקשרות, פרטי נסיעותיו והרגלי הפרט במהלך חיי היומיום, פרטים פיננסיים, התייחסות למוגבלות ועוד. מידע זה הוא, לכל הפחות בחלקו, "מידע רגיש" כהגדרתו בסעיף 7 לחוק הגנת הפרטיות.

מצב זה מעלה את החשש כי המידע שייאסף במסגרת השימוש ביישומונים יזלוג וייחשף בפני גורמים שאינם מורשים. לאור כך שהמידע הנאסף הוא מידע רגיש הכולל פרטים מזהים, ואשר מתוכו ניתן גם ללמוד רבות על התנהלותו של אדם ועל אורחות חייו, הרי שזליגת מידע במצב שכזה עלולה להוות פגיעה קשה וחמורה בפרטיות.

בעניין זה יש לציין כי שימוש ביישומונים, על-אף היתרונות הרבים שיש בו, עלול להיות בעייתי מבחינת הגנה על פרטיות, וזאת מעצם היותם פועלים תחת מכשירים חכמים המאפשרים לגורמים שונים גישה למידע הנמצא בהם. כך, כפי שנכתב בדו"ח של מרכז המידע והמחקר של הכנסת משנת 2016 שדן בהיבטי פרטיות ביישומונים, "סביבת המשתמש של הטלפון החכם מבוססת על מספר לא מבוטל של ספקי שירות בשכבות שונות של המוצר: החברה המייצרת את החומרה – הטלפון עצמו; החברה המפתחת את מערכת ההפעלה שעל גביה פועל המכשיר; חברות התקשורת המפעילות (ספקי שירותי השיחות והגישה לאינטרנט); חנויות האפליקציות; מפתחי האפליקציות ולבסוף צדדים שלישיים שונים (רשתות מפרסמים ועוד). **לכל גורם בשרשרת האמורה יכולה להיות השפעה על פרטיות המשתמש"** (ההדגשה במקור).[4]

כך לדוגמה, חיבור מכשיר חכם לרשת אלחוטית (Wi-Fi) ציבורית עלול לחשוף מידע השמור בטלפון לגורמים שונים ה"יושבים" על אותה רשת. במובן זה, בניגוד לכרטיס חכם, אשר אינו חשוף במובנים אלו, שימוש ביישומונים לתשלום ותיקוף שימוש בתחבורה ציבורית חושף את המשתמשים בהם בצורות שונות ונרחבות יותר, העשויות להביא לזליגת מידע רגיש על אודות המשתמשים.

בנוסף לכל האמור יש לזכור כי בטלפונים חכמים נשמר מידע רב על אודות המשתמשים בהם, שאינו נובע מהשימוש ביישומונים של התחבורה הציבורית. מידע זה כולל, בין היתר, את היסטוריית החיפוש במנועי החיפוש שבטלפון, תכתובות הדוא"ל, הודעות טקסט ותמונות. מידע זה הינו רגיש במהותו ויש בו בכדי ללמד רבות על זהותו של בעל הטלפון ואורחות חייו. מטבע הדברים, שילוב מידע זה עם מידע הנובע מהשימוש ביישומונים, מגביר את פוטנציאל הפגיעה בפרטיות, במידה ומידע זה יזלוג ויגיע לגורמים לא מורשים. במובן זה, שימוש ביישומונים מגביר את פוטנציאל הפגיעה בפרטיות הקיימת מלכתחילה בשימוש במכשירים חכמים. יצוין, כפי שיפורט בהמשך, כי מקום בו נעשה עיצוב מוכוון פרטיות מושכל מראש, ניתן לייצר איזונים מתאימים למתן מענה לשימוש ביישומונים.

4 מרכז המחקר והמידע של הכנסת "סוגיית הפרטיות בטלפונים החכמים" 2 (18.7.2016), https://m.knesset.gov.il/News/PressReleases/Documents/190716.pdf.

- **אבטחת המידע –** בהמשך ישיר לנקודה הקודמת יש לציין כי מגוון השיטות השונות בהן יישומונים אוספים מידע לגבי שימוש בתחבורה החכמה ומתקפים את השימוש בתחבורה הציבורית, יכול להוות ווקטור תקיפה מצידם של גופים המעוניינים לשבש את פעילות היישומונים, את מערכות התחבורה החכמה או את מאגרי המידע שבהן. גופים כאלה פועלים גם לשם גניבת מידע אודות המשתמשים ביישומון, לרבות תוך ניסיון להונות אותם או את המערכת לשם הוצאת כספים וגניבתם. כך לדוגמה, תוקפים עלולים לנצל את השימוש במערכות מבוססות NFC כדי לדמות סריקה של מכשיר טלפון על ידי קורא נייד במהלך הליכה במרחב הציבורי. במהלך פעולה כזו יועברו פרטי מידע לסורק הנחזה להיות מותקן בתחבורה ציבורית, ובהמשך עלולות אף להתבצע טרנזאקציות פיננסיות. כל האמור מחדד את הצורך ביישום מערכות מתקדמות לאבטחת מידע.
- **איסוף מידע שלא לצורך –** שימוש ביישומונים לתשלום ולתיקוף שימוש באמצעי תחבורה ציבורית עשוי להביא למצב בו מידע אישי רב על אודות משתמשים – לרבות כזה אשר אינו נדרש לשם מתן השירות (כגון מקום מגוריו של אדם) – ייאסף ויישמר במאגרי מידע שונים, וזאת לפרקי זמן ארוכים, וללא כל תכלית ראויה. בעניין זה יש לזכור כי בעבור אנשים רבים, השימוש בתחבורה ציבורית נעשה ברמה יומיומית, וכן כי מידע על אודות הרגלי הנסיעה של אדם בתחבורה הציבורית עשוי, מעצם טבעו, להוות בסיס לחשיפת מידע נוסף על אודות אותו אדם. כל האמור מחדד את הבעייתיות שבאיסוף מידע עודף במסגרת שימוש ביישומונים האמורים.
- **הרשאות גישה למכשירים ואמצעים טכנולוגיים נוספים –** בהמשך לנקודה הקודמת יש לזכור כי יישומונים רבים מבקשים מהמשתמשים בהם הרשאות גישה למידע המצוי במכשיר החכם (כגון לרשימת אנשי הקשר שלהם או למאגר התמונות שבמכשיר) ולאמצעים טכנולוגיים נוספים הקיימים בו (כגון מצלמה, מיקרופון וכדומה). הרשאה זו, הניתנת במקרים רבים על-ידי משתמשים מבלי שנתנו את מלוא דעתם להשלכותיה, חושפת אותם בצורות שונות, ועלולה להביא לכך שמידע רגיש על אודותיהם ייאסף ויעובד לצרכים שונים, כתוצאה מהרשאה זו. במקרים רבים ההרשאה המבוקשת אינה מחויבת לשם מתן השירות עצמו. כך לדוגמה, יישומון לניווט גיאוגרפי המבוסס GPS אינו יכול לפעול ללא הרשאה לנתוני המיקום של המכשיר. מנגד, הרשאה למצלמה או למיקרופון (הגם שיכולים להיות רלוונטיים ליכולות מסוימות של היישומון), אינם מחויבים לשם פעילותו הבסיסית.
- **שימוש במידע למטרות זרות ופסולות –** לאור רגישותו של המידע הצפוי להיאסף במסגרת היישומונים וערכו הכלכלי, קיים חשש כי גורמים בעלי אינטרסים יבקשו לעשות שימוש במידע למטרות זרות ופסולות, וזאת כחלק מהניסיון להתחקות אחר התנהלותו של אדם ואורחות חייו. שימוש שכזה במידע מהווה, מטבע הדברים, פגיעה חמורה בפרטיות. בעיה זו מתחדדת שעה שהגורמים האמונים על איסוף המידע ועיבודו הם גורמים פרטיים בעלי עיסוקים ואינטרסים כלכליים, העלולים ליצור להם תמריץ לעשות שימוש במידע גם לשם הפקת רווח כלכלי.

עמדת והמלצות הרשות להגנת הפרטיות

עמדתה העקרונית של הרשות להגנת הפרטיות היא כי פרטיות אינה מהווה חסם בפני השימוש באמצעים דיגיטליים המבקשים להביא לייעול השירותים הציבוריים ולחסכון במשאבי הציבור. **עם זאת, קידום אמצעים דיגיטליים ויישומם צריך להיעשות בצורה הוגנת, מאוזנת, סבירה, בטוחה ושקופה, תוך מתן התייחסות מעמיקה להיבטים של הגנה על פרטיות.** זאת במיוחד כאשר מדובר באמצעים דיגיטליים האמורים להיות מיושמים למתן ולהספקת שירותים ציבוריים חיוניים.

ככלל, השימוש ביישומונים לתשלום ותיקוף שימוש בתחבורה ציבורית אינו פסול מיסודו ואין בו, שלעצמו, בכדי להוות פגיעה בפרטיות. **עם זאת, לאור היות התחבורה הציבורית שירות ציבורי חיוני, לאור האתגרים שפורטו קודם לכן, ובמיוחד לאור העובדה כי במקרים רבים לא עומדות בפני היחיד חלופות אחרות פרט לשימוש בשירותי תחבורה ציבורית – הרי שיש להקפיד כי השימוש ביישומונים לתשלום ולתיקוף שימוש בתחבורה ציבורית ייעשה תוך הגנה על פרטיות המשתמשים.**

לאור האמור ולאור כל שפורט לעיל, הרשות להגנת הפרטיות מבקשת לחדד את הנקודות הבאות:

- שימוש ביישומונים לתשלום ולתיקוף השימוש בתחבורה ציבורית כרוך באיסוף ובעיבוד של מידע אישי רגיש שיש בו פוטנציאל להביא לפגיעה חמורה בפרטיותם של משתמשי התחבורה הציבורית בישראל.
- על משרד התחבורה וכל גוף או רשות ציבורית, המתקשרים עם הגורמים המפעילים והמספקים את היישומונים לצורך מתן שירות ציבורי חיוני, ובמקרה הנדון לתשלום ולתיקוף השימוש בתחבורה ציבורית, מוטלת האחריות לוודא כי גורמים אלו פועלים בהתאם להוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.
- בהתאם להוראות סעיף 17 לחוק, על משרד התחבורה ועל הגורמים המפעילים והמספקים את היישומונים לעמוד בהוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, לרבות בכל הנוגע לחובות המוטלות עליהם בהיבטים של אבטחת מידע ואופן ניהול מאגרי המידע. בהתאם לאמור לעיל, אבטחת המידע צריכה להיעשות, ככל האפשר, ביחס לכל השלבים בשרשרת השימוש ביישומונים (קרי מרגע ההורדה מחנות היישומונים ועד לאופן השימוש בהם בפועל), ותוך מתן התייחסות מיוחדת לאתגרים הייחודיים הקיימים בנושא, כמו לדוגמה בכל הנוגע לחשיפת מידע המצוי בטלפון החכם במסגרת גלישה ברשת ציבורית ו"פתוחה".
- חשוב לוודא כי הליך קבלת הסכמת משתמשי התחבורה הציבורית לשימוש ביישומונים ולאיסוף המידע ייעשה באופן המאפשר למשתמשים לקבל את כל המידע הנדרש להם לשם מתן הסכמה מדעת, באופן פשוט וקל להבנה. התייחסות מיוחדת יש להעניק בהקשר זה לאוכלוסיות רגישות כגון קשישים, ילדים ואנשים עם מוגבלות.

- **מומלץ כי הגורמים הרלוונטיים (משרד התחבורה והגורמים המספקים את השירות) יעמידו בפני ציבור משתמשי התחבורה הציבורית את האפשרות להשתמש ביישומונים במידה כזו או אחרת של אנונימיות**, ככל שדבר זה אפשרי מבחינה טכנולוגית. בכך יתאפשר למשתמשים לשלוט על פרטיותם ולבחור בין שימוש הכרוך באיסוף מידע אישי לכזה המאפשר להם לשמור על אנונימיות במסגרת השימוש. מודל שכזה מיושם בישראל במסגרת שימוש בכרטיס ה-"רב-קו". נדגיש כי אפשרות מעין זו צריכה להיות חלק מהמפרט הטכנולוגי הראשוני של היישומונים, חלק מעיצוב מכוון פרטיות.
- במידה שלמשתמשים לא תעמוד האפשרות לשימוש אנונימי ביישומונים, **חשוב לוודא כי במקביל תמשיך לעמוד לציבור חלופה סבירה וממשית לשימוש בהם, כגון שימוש בכרטיס חכם אנונימי או תשלום במזומן.** אי-הצגת חלופה תכפה על ציבור המשתמשים לתת הסכמתם לאיסוף המידע, באופן המנוגד למהותו של עיקרון ההסכמה והוראות סעיף 1 לחוק הגנת הפרטיות.
- יש לוודא כי הגורמים האוספים מידע במסגרת השימוש ביישומונים עושים שימוש במידע שנאסף אך ורק בהתאם למטרה שהוגדרה מלכתחילה במסגרת קבלת ההסכמה לאיסוף המידע.
- יש לוודא כי המידע הנאסף במסגרת השימוש ביישומונים הוא רק כזה הנדרש לצורך הפעלת שירות התחבורה הציבורית. ככל שהגורם המפעיל את היישומונים מבקש לאסוף מידע מהמשתמשים לשימושים נוספים ולמטרות שאינן הפעלת שירות התחבורה – יש להקפיד כי איסוף מידע זה ייעשה רק לאחר קבלת הסכמה אקטיבית (Opt-in Mechanism) של המשתמשים לשימושים ומטרות אלו.
- מומלץ כי ההסכמה לשימושים נוספים תעשה, ככל הניתן, בהליך נפרד מהליך בקשת ההסכמה הראשונית לעצם השימוש ביישומונים לצרכי נסיעה בתחבורה הציבורית. כמו כן אין להתנות את השימוש ביישומונים בקבלת הסכמה לאיסוף מידע לשימושים נוספים. בעניין זה **יש להבהיר למשתמשים כי סירובם להעניק את ההסכמה לשימושים הנוספים לא יפגע בהם ולא ישפיע על אפשרות שימושם ביישומונים לצורכי נסיעה בתחבורה ציבורית.**
- מומלץ כי במסגרת השימוש ביישומונים לא יידרשו המשתמשים להעניק הרשאת גישה למידע המצוי במכשיר החכם או לאמצעים טכנולוגים המותקנים בו (מצלמה, מיקרופון), אלא רק להרשאות הבסיסיות הנדרשות לפעילות תקינה של המכשיר והיישומון. ככל שהגורם המפעיל את היישומונים מבקש הרשאה למטרות אחרות – עליו להבהיר למשתמשים כי הרשאה זו אינה נדרשת לעצם פעילות היישומון ולהסביר להם את משמעות מתן ההרשאה מבחינת ההגנה על פרטיותם. כמו כן, יש להבהיר למשתמשים כי סירוב להענקת הרשאות לשימושים/אמצעים שאינם מחויבים לפעילות היישומון, לא יפגע או ישפיע על היכולת להשתמש ביישומון לצורכי נסיעה בתחבורה ציבורית.

- בהתאם לתקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, יש לוודא כי הגורמים שמאגרי המידע מצויים בבעלותם (בעל המאגר) יבחנו, לפחות אחת לשנה, אם המידע הנשמר על-ידם בהקשר זה אינו חורג מהנדרש ביחס למטרות המאגר.
- ככל שמידע הנאסף אמור לעבור לתחומי מדינה אחרת יש לוודא עמידה בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.
- רצוי כי קידום התהליכים הטכנולוגים להטמעה ולשימוש ביישומונים בתחבורה הציבורית ייעשה תחת מסגרת של עיצוב לפרטיות (Privacy by Design), אשר יבחן את אופן ההגנה על פרטיות, לרבות ברמה טכנולוגית, כבר בשלב תכנון האמצעים השונים. תהליך זה קריטי במיוחד כאשר עסקינן באמצעים טכנולוגיים האמורים לפעול במסגרת הספקת שירותים ציבוריים חיוניים, ושיישומם כרוך באיסוף ועיבוד מידע אישי.
- יש לוודא כי לציבור המשתמשים תעמוד הזכות לעיין במידע הנוגע אליהם אשר נאסף במסגרת שימוש ביישומונים, ואף לדרוש את תיקונו, והכל בהתאם להוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.
- רצוי כי אופן השימוש במידע הנאסף יהיה, במידת האפשר, שקוף לכלל הציבור.

מידע אישי ברכב הפרטי שלך – מבט לעתיד

התפתחות תחום התחבורה החכמה מביאה להקמת שירותים רבים שאוספים ומשתפים מידע על משתמשים וסביבתם. ספקים נותני שירות אלה נדרשים לעמוד בהוראות דיני הגנת הפרטיות, אותן ניתן לבחון בהסכם השימוש והמדריך המצורף לשירות אצל כל ספק. על רכבים כיום מותקנות מערכות ותוספים שונים שמסתמכים על איסוף מידע ושימוש בנתונים שמטרתם לתמוך בנסיעה בטוחה, יעילה, נוחה וחווייתית. מטרת פרק זה היא לספק הצצה למגמות ולטכנולוגיות הצפויות להשפיע על השימוש במידע האישי ברכב הפרטי בעתיד הקרוב. העקרונות והכללים המפורטים במדריך זה יחולו, בשינויים המחויבים, גם ביחס למגמות וטכנולוגיות עתידיות אלו.

איסוף נתונים על ידי רכבים

הנתונים שנאספים כיום על ידי כלי הרכב, קשורים בעיקר לנסיעה ולתפקוד הרכב במסגרתה:

- **ניטור נתוני נסיעה (EDR)** – מערכת לניטור נתונים טכניים בזמן הנהיגה ברכב. המערכת מותקנת ברוב הרכבים הקיימים כיום בשוק. היא מאפשרת קבלת מידע לפני ולאחר תאונה – כגון מהירות הרכב, שימוש בחגורות בטיחות, שימוש בבלמים ועוד.
- **On-Board Diagnostic Information (OBD)** – שקע פיזי אליו ניתן לחבר מחשב ייעודי או רכיבים אלקטרוניים שונים שמתחברים למחשב הרכב על מנת לקבל מידע או לבצע פעולות בתוכנות הרכב.

טכנולוגיות חדשות שמתפתחות ויכנסו בעתיד הקרוב לרכבים

התפתחות הרכב האוטונומי, המקושר, החשמלי והשיתופי – מובילה לאיסוף מידע רב ממגוון מקורות וסוגים הנוגעים לנסיעה ברכב, כגון זהות הנהג, הנוסעים והסביבה. בין הנתונים שנאספים במסגרת מערכות אלה ניתן לכלול:

- **מיקום** – על ידי לוויין (GPS) או חיבור לרשתות סלולריות אחרות.
- **סביבה קרובה** – על ידי חיישנים שונים כגון מצלמות, חיישני תנועה וקול שמטרתם לקלוט את הסביבה הקרובה לרכב ולסייע לנהג בפעולות דוגמת מעבר נתיב, זיהוי רכבים קרובים ונהיגה בטוחה.
- **שירותים בתוך הרכב** – מצלמות, מיקרופונים וחיישנים בתוך תא הנהג והנוסעים עשויים לאסוף מידע במסגרת שירותים שונים כמו שימוש בטלפון, זיהוי נוסעים לצרכים שונים (פתיחת כריות אוויר אופטימלית למשל) או יצירת קשר במצב חירום.
- **זיהוי משתמש** – כלים לזיהוי ביומטרי של הנהג: תמונה, סריקת פנים, טביעת אצבע ועוד עשויים לאסוף מידע במסגרת שירות להתאמת הרכב לנהג וכן לצורכי אבטחה. איסוף שכזה עשוי להתבצע גם במסגרת שירותי סיוע לנהג דוגמת סריקת עיניים ומבט לזיהוי מצבי עייפות.

- **אפליקציות** – איסוף מידע באמצעות אפליקציות צד שלישי, שנועדו לשירותי תוכן ושירותי נסיעה שמאפשרים בחלקן התממשקות למערכות הרכב.

הרשאות נוספות ברכב הפרטי שלך

- **סנכרון טלפון אישי או פרטי משתמש ללקוחות ספקי המידע השונים (גוגל, אפל, פייסבוק וכו')** – סנכרון משתמש או טלפון יכולים לאפשר למערכת ולשירותים חיצוניים גישה לנתונים שונים: אנשי קשר, שיחות, הודעות, ספריית מדיה, מצלמה, מיקרופון, מיקום, יומן, היסטוריית חיפוש, יומן, סורק ביומטרי ועוד.
- **אישור להעברת מידע** – העברת מידע לגורמים שונים ולצרכים מגוונים. כך למשל, העברת מידע בנוגע לנתוני הרכב ומיקומו אל יצרן הרכב.
- **אישור לעיבוד המידע** – שימוש בנתונים לעיבוד נוסף ויצירת סטטיסטיקות או הפקת תובנות מעבר לשימוש הבסיסי בשירות.
- **אישור לשליחת דיוור ישיר** – מתן הרשאה לקבל פניות דיוור ישיר, פניות ישירות ללקוח על בסיס מאפייני קבוצות שונות (מין, גיל, מגורים, העדפות וכו'). (הרחבה בדף מידע – דיוור ישיר).

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة القانون التكنولوجيا والمعلومات

073-3928555 | PPA@justice.gov.il | WWW.PPA.JUSTICE.GOV.IL

קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | חפשו אותנו גם בפייסבוק