הנחיית הרשות להגנת הפרטיות מס' 1/2012

תחולת הוראות חוק הגנת הפרטיות על מאגרי מידע של מפעילי כרטיס חכם בתחבורה ציבורית

נוסח מעודכן בעקבות תיקון 13

1. מטרה

1.1. בהתאם להחלטת משרד התחבורה, נעשה על ידי חברות התחבורה הציבורית מעבר משימוש בכרטיסי נייר בתחבורה הציבורית לשימוש בכרטיס אלקטרוני הניתן לטעינה (להלן - **כרטיס חכם**).

1.2. מטרת הנחיה זו להציג את עמדת הרשות להגנת הפרטיות (להלן - **הרשות**) באשר לתחולת הוראות חוק הגנת הפרטיות, התשמ"א - 1981 (להלן - **החוק**) על איסוף עיבוד ושימוש במידע באמצעות כרטיס חכם למאגרי מידע של מפעילי כרטיס חכם בתחבורה ציבורית (לרבות מול מרכז שירות ארצי, כמפורט להלן, ככל שפעילותו רלוונטית כבר למפעיל) ולהנחות את חברות התחבורה הציבורית המפעילות כרטיס חכם באשר להתאמה להוראות החוק.

1.3. בכל הנוגע להיבטי פרטיות באפליקציות תשלום בתחבורה ציבורית, ראו מסמך ייעודי שפרסמה הרשות להגנת הפרטיות בשנת 2020 בנושא "**היבטי פרטיות ביישומונים (אפליקציות) לתשלום ותיקוף שימוש בשירותי תחבורה ציבורית**".[1]

2. רקע עובדתי

2.1. לפני מספר שנים, במטרה לבסס אמצעי תשלום אחיד בכלל שירותי התחבורה הציבורית בישראל (אוטובוסים, רכבת, רכבת קלה), החל משרד התחבורה לחייב את חברות התחבורה הציבורית לעבור לשימוש בכרטיס חכם, המכונה "רב-קו".

2.2. הסדרת פעילות חברות התחבורה הציבורית (להלן - מפעילי כרטיס חכם) בהקשר של הפעלת כרטיס חכם נעשתה בין היתר בהסכם שנחתם בין משרד התחבורה לבין כל אחד מהמפעילים בנפרד (להלן – **ההסכם**).

[1] הרשות להגנת הפרטיות "היבטי פרטיות ביישומונים (אפליקציות) לתשלום ותיקוף שימוש בשירותי תחבורה ציבורית" (2020). המסמך זמין כאן.

2.3. במקביל, בכוונת משרד התחבורה להסדיר נושא זה באמצעות חקיקה בצורה מפורטת וברורה יותר.[2] עוד מתוכננת הקמת מרכז שירות ארצי שיספק, בין היתר, שירותי סליקה וקיזוז של תביעות הדדיות בין מפעילים לעניין הפדיון ששולם תמורת נסיעות וייתן שירות לציבור המשתמשים בכרטיסים חכמים ולמנפיקים של כרטיסים חכמים (להלן – **מרכז השירות**).

2.4. <u>איסוף מידע על ידי מפעיל כרטיס חכם</u>

2.4.1. לפי ההסכם הנ"ל, כאשר נוסע מבקש כי יונפק לו כרטיס חכם הכולל הנחות ייעודיות לקבוצת אוכלוסייה מסוימת, מפעילי הכרטיס החכם אוספים את הנתונים הבאים, כולם או מקצתם (לפי המקרה): תמונה צבעונית, מספר תעודת זהות, שם משפחה, שם פרטי וסוג זכאות הנוסע ("פרופיל הנוסע"), תאריך לידה, כתובת למשלוח דואר, מספר טלפון נייד, מספר טלפון בבית, כתובת דואר אלקטרוני, שם חברה, מספר עובד (להלן – **מידע אישי אודות הנוסע**). בנוסף, באפיון שערך משרד התחבורה לשדות מידע אודות אוכלוסיות ייעודיות שניתן לכלול בכרטיס החכם פורטו נתונים כגון חייל, סטודנט, נכה, חירש, עיוור, ילד, קטין, זכאי ביטוח לאומי ועוד.

2.4.2. בבדיקת פעילות מפעילי הכרטיס החכם במסגרת הליכי פיקוח שביצעה הרשות, התברר, כי נוסף על הנתונים המפורטים לעיל המפעילים השונים אוספים, לעיתים, גם נתונים נוספים דוגמת מין, שם מוסד לימודים, כתובת מוסד לימודים.

2.4.3. בנוסף, נאספים במסגרת הפעלת המערכת נתוני שימוש בכרטיס כגון מספר הקו, מספר כלי התחבורה בו בוצעה הנסיעה, תחנת העלייה על כלי התחבורה, תאריך ושעת העלייה.

2.4.4. המידע הנאסף במסגרת הפעלת כרטיס חכם נשמר במספר מקומות:

2.4.4.1. במאגר מידע שברשות כל אחד מהמפעילים נשמר כל המידע האישי ביחס לכרטיס החכם, כולל מידע אישי שנמסר ישירות על ידי הנוסע ומידע שנאסף מעמדות הכרטוס בכלי התחבורה השונים;

2.4.4.2. בעמדות הכרטוס בכלי התחבורה השונים נשמר מידע לגבי הכרטיסים בהם נעשה שימוש באותו כלי תחבורה;

2.4.4.3. בשבב שעל גבי הכרטיס החכם נשמר מידע אישי על הנוסע וכן מידע על נסיעות שבוצעו באמצעות הכרטיס (בהיקף מוגבל כפי יכולות הכרטיס);

[2] ראו את הצעת חוק לתיקון פקודת התעבורה (מס' 100) (רישיון מפעיל וכרטיס חכם), התשע"א - 2010 ה"ח 541.

2.4.4.4. במשרד התחבורה נשמר מידע שנאסף מהמפעילים השונים על הנפקת כרטיסים חכמים והשימוש בהם.

2.4.4.5. מהאמור לעיל עולה, כי במסגרת הפעלת כרטיס חכם נאסף מידע אישי במאגר מידע, שעשוי לכלול גם "מידע בעל רגישות מיוחדת", כהגדרתו בסעיף 3 לחוק.

2.5. <u>אבטחת המידע הנאסף על ידי מפעילי כרטיס חכם</u>

2.5.1. לפי ההסכם, מחויבים המפעילים לקיום נהלי עבודה ומערכת בקרה על מנת למנוע שימוש לרעה במידע האישי הנאסף בעמדות ההנפקה (המופעלות על ידם), ונדרשים למסור דיווח על תפעול עמדות ההנפקה, כולל כניסות ויציאות מורשי גישה למערכת.

2.5.2. לפי סעיף 17 לחוק, על מפעילי כרטיס חכם חלה האחריות לאבטחת המידע במאגר המידע. כך, גם לפי ההסכמים בין משרד התחבורה לבין מפעילי הכרטיס החכם, נדרשים המפעילים למנגנוני אבטחה ובקרה.

3. ההנחיה

3.1. כאמור לעיל, בעת הנוכחית מפעילי כרטיס חכם אוספים מידע רגיש מדרגות שונות, החל במין הנוסע, המשך בפרופיל הנוסע (היכול להעיד על מצבו הכלכלי או מצב בריאותו) וכלה בנתונים הנאספים על המיקומים בהם שהה, כגון תחנת עליה, המאפשרים מעקב פיזי אחר הנוסע (להלן – "**נתוני מיקום**"). להלן תוצג עמדת הרשות להגנת הפרטיות לעניין תחולת הוראות חוק הגנת הפרטיות על מאגרי מידע של מפעילי כרטיס חכם בתחבורה ציבורית:

3.1.1. מפעילי כרטיס חכם עושים שימוש במאגר מידע, המכיל מידע בעל רגישות מיוחדת כמשמעו בסעיף 3 לחוק. לפיכך, ככל שמספר בני האדם שיש על אודותיהם מידע בעל רגישות מיוחדת במאגר מידע עולה על 100,000, חלה על מפעילי הכרטיס החכם חובת הודעה לרשות להגנת הפרטיות אודות מאגר המידע, בצירוף מסמך הגדרות המאגר לפי סעיף 8א(ב) לחוק;

3.1.2. מטרת המאגר שתרשם במסמכי הגדרות המאגר של המפעילות, הנה "איסוף מידע לצורך ניהול כרטיסים חכמים לתחבורה ציבורית ומתן שירות ללקוחות ביחס אליהם". יובהר כי חל איסור על שימוש במידע הנאסף למטרות אחרות, ובכלל זה מטרות שיווק או מטרות אחרות של מפעיל התחבורה הציבורית.

3.1.3. <u>מימוש עקרון המידתיות – אי כבילה בין נסיעה בתחבורה ציבורית לאיסוף מידע (כרטיס אנונימי)</u>

3.1.3.1. עקרון המידתיות, הנובע מהיותה של הזכות לפרטיות זכות יסוד חוקתית המעוגנת בחוק יסוד: כבוד האדם וחירותו, מחייב כי בפני נוסע המעוניין לעשות שימוש בתחבורה הציבורית תהיה האפשרות לקבל את השירות באופן שפגיעתו בפרטיות תהיה הקטנה ביותר. משכך, יש להעמיד לרשות הנוסעים חלופה אנונימית לכרטיסים החכמים המזוהים, שבמסגרתה לא נאסף כל מידע אישי על אודות הנוסע (במאגר מידע או בשבב שעל הכרטיס).

3.1.3.2. על חלופה זו להיות חלופה ממשית, שאינה נחותה משמעותית ביחס לכרטיסים המזוהים, אלא אם כן קיימים טעמים חזקים לכך שסוגים שונים של הסדרי נסיעה יתאפשרו רק לאחר מסירת פרטים אישיים שיישמרו במאגר מידע או על גבי השבב. זאת על מנת שניתן יהיה לייחס הסכמה מדעת לאותם נוסעים שבחרו בחלופות המזוהות. שכן אם לנוסע אין אפשרות בחירה אמיתית אזי הדבר משליך על יכולתו ליתן הסכמה מדעת.

3.1.3.3. לעניין זה, עמדת הרשות הינה כי, ככל שניתן, ובהעדר טעמים מנוגדים כאמור לעיל, יש להציע חלופות אנונימיות **לכל סוגי הכרטיסים החכמים המוצעים**, בכפוף לגיבוש הסדרים שמטרתם לדאוג למניעת הונאות. לדוגמא, לעניין כרטיסים מסוג "חופשי חודשי", נבחנת האפשרות להסתפק בכרטיס שעל גביו מודפסים שם הנוסע, תמונתו ומספר הזיהוי שלו, והמידע האישי אינו נשמר במאגר ממוחשב או בשבב של הכרטיס.

3.1.3.4. בנוסף, יש להבחין בין שימוש בפרטים מזהים ופרטים אודות זכאות, שעשויים להיבדק בשלב הנפקת הכרטיס, לבין הפרטים המוזנים לשבב של הכרטיס החכם. יש להעדיף פתרון שבו, ככל שנדרשים פרטים מזהים, אלה יודפסו על גבי הכרטיס, אך לא יוזנו לשבב. זאת משום שפרטים שאינם מוזנים לשבב, אינם נתונים לעיבוד ממוחשב בעת השימוש בתחבורה ציבורית.[3]

3.1.3.5. בהתאם לכך אין להזין לשבב כל פרטים אישיים.

3.1.3.6. בידי הרשות ממצאים כי כיום מבנה הנתונים בכרטיס החכם מכיל תעודת זהות. בהתאם לכך, עד לתיקון נושא זה, בפרקי הזמן שייקבעו, יש להמנע משימוש שגרתי בנתון בזה, ולהגביל את יכולת הקריאה שלו, ככל הניתן.

[3] לעניין השימוש במספר תעודת זהות כפגיעה בפרטיות, ראו: בג"צ 6824/07 **מנאע נ' רשות המסים** (2010), פסקה 37. ראו גם גילוי הדעת של הרשות להגנת הפרטיות בנושא "איסוף מספרי תעודות זהות וצילום תעודות זהות" (2024). זמין כאן.

3.1.4. <u>קבלת הסכמה מהנוסע</u>

3.1.4.1. לצורך איסוף מידע על נוסע ואודות השימוש בו, **יש לקבל מהנוסע הסכמה, כמשמעה בסעיף 3 לחוק.**

3.1.4.2. עמדת הרשות כי ככל שנדרש זיהוי הלקוח לצורכי שירות הקשורים בכרטיס הרב קו עצמו, כגון הסדר המאפשר שיחזור נסיעות במקרה של אובדן, מותר לאסוף פרטי קשר של נוסע. אולם פרטי קשר אלה צריכים להיות בהיקף המינימלי ביותר הנדרש. אין צורך באיסוף כל פרטי המידע המפורטים לעיל.

3.1.4.3. בהתאם לכך, יש להבהיר ללקוח כי הפרטים נדרשים לשם יצירת קשר איתו בלבד, ולכן זכותו למסור פרטים בהיקף שהוא מבקש בלבד. הוא רשאי לבחור למסור אחד או יותר מאלה: כתובת, מספר טלפון, מספר טלפון נייד, או כתובת דואר אלקטרוני, ואינו חייב למסור את כל הפרטים הנ"ל.

3.1.4.4. במקרים שבהם הדבר נדרש, כגון שהכרטיס נקנה בידי מעביד, או משולם בידי מעביד, ניתן לאסוף גם מידע זה בטופס ההרשמה.

3.1.4.5. **יודגש כי ככל שמפעיל תחבורה ציבורית מעוניין להקים מועדון לקוחות או לבצע פעולות שיווקיות אחרות הקשורות באיסוף מידע אישי מהציבור, חל איסור לקשור בין איסוף זה לבין איסוף לצרכי הרב קו. על האיסוף לצרכי הרב קו להיות נפרד לחלוטין מהאיסוף לצרכים שיווקיים. כך גם הורה משרד התחבורה במסגרת ההסכם.**

3.1.4.6. בהתחשב בכך שתחבורה ציבורית מהווה מצרך חיוני ונוסע המבקש לעשות בו שימוש מחויב לעשות זאת באמצעות כרטיס חכם, **נדרשת הסכמה מדעת (כלומר כזו שהלקוח הסכים לה לאחר שנמסר לו מידע על כך) לשימוש במידע. הסכמה כאמור על ידי הנוסע יכול שתינתן רק לגבי המידע האישי החיוני לאספקת שירות התחבורה הציבורית ורק לגבי שימוש במידע למטרות הנדרשות במישרין לאספקתו.**

3.1.4.7. על ההסכמה הניתנת על ידי הנוסע להיות הסכמה מדעת, תוך קיום חובת היידוע לפי סעיף 11 לחוק.

3.1.4.8. לצורך קבלת הסכמה מדעת, ובהתאם להוראות סעיף 11(1) לחוק, יש להציג בפני הנוסע, במעמד ההנפקה, את חלופת הכרטיס האנונימי העומדת לרשות הנוסעים. **לשם כך, יש לדאוג שהחלופה של הפקת כרטיס חכם אנונימי תובלט בשילוט בעמדות ההנפקה, באתרי האינטרנט של המפעילים ובמסגרת הדרכת נותני השירות בעמדות ההנפקה**. במסגרת זו, יש ליידע את הנוסע על כך שבמידה שבחר בחלופה האנונימית, יתכן שלא יוכל לממש הנחות מסויימות בדמי הנסיעה ולא יוכל לשחזר את הכרטיס או את היתרה שנטענה בו במקרה של אובדן, גניבה או תקלה בכרטיס.

3.1.4.9. **ביחס לנוסע שהוא קטין**, ההסכמה מדעת לאיסוף המידע האישי והשימוש בו יכולה להינתן רק על ידי מי שהוא האפוטרופוס של הקטין. ככל הניתן, המידע האישי הנשמר במאגר יתייחס לאפוטרופוס של הקטין ולא לקטין עצמו. לגבי קטין מגיל 14 ומעלה יש לבקש **גם** את הסכמת הקטין עצמו.

3.1.4.10. ביחס לנוסע שהוא קטין, המידע אותו המפעיל רשאי לאסוף לצורך הנפקת כרטיס מזוהה לקטין הוא המידע הבא בלבד: שם הקטין, מספר תעודת הזהות של האפוטרופוס נותן ההסכמה וכן תאריך סיום הזכאות לקטין (במקום תאריך הלידה של הקטין, הנדרש היום).

3.1.4.11. בנוסף, ורק על בסיס הבהרה מפורשת כי מדובר בחלק שהינו רשות ולא חובה, ניתן לקבל מספר טלפון של האפוטרופוס נותן ההסכמה, לצורך יצירת קשר לשם שחזור הכרטיס במקרה אובדן.

3.1.4.12. מהאמור נובע גם שלא ניתן להניח כי מי שמעונין להשתמש בתחבורה הציבורית מעוניין בהכרח להיכלל ב-"מועדון לקוחות" של מפעיל התחבורה הציבורית או כי ייעשו עיבודים נוספים הקשורים במידע האישי שלו, כגון שיווק או דיוור ישיר, **ללא קבלת הסכמה מפורשת ונפרדת**. הסכמה נפרדת זו **לא תהווה תנאי למתן שירות התחבורה הציבורית לנוסע ויש לאפשר לו לבטלה בכל עת.**

3.1.5. <u>מטרות השימוש במידע הנאסף באמצעות כרטיס חכם</u>

3.1.5.1. המידע האישי הנאסף על ידי מפעיל כרטיס חכם משמש הן את המפעיל עצמו והן את משרד התחבורה. להלן תפורט עמדת הרשות באשר למטרות השימוש במידע זה.

3.1.5.2. <u>שימוש במידע על ידי משרד התחבורה</u>

3.1.5.2.1. ככלל, המטרה לשמה נדרש משרד התחבורה לעשות שימוש במידע האישי שנאסף באמצעות כרטיס חכם הינה לצרכי מימוש תפקידו.

3.1.5.2.2. לצורך מטרה זו, המידע הנדרש למשרד התחבורה הוא מידע בלתי מזוהה (מידע סטטיסטי) בלבד.

3.1.5.2.3. כמו כן, ייתכן כי במסגרת ביצוע פעולות פיקוח אצל המפעילים ובירור תלונות שהוגשו כנגדם, משרד התחבורה עשוי להידרש למידע מזוהה לצורך מטרות אלה.

3.1.5.2.4. בנוסף, בעתיד במסגרת שירותי מרכז השירות עשוי משרד התחבורה להידרש למידע מזוהה.

3.1.5.3. <u>שימוש במידע על ידי המפעילים</u>

3.1.5.3.1. מפעיל כרטיס חכם יכול לבצע שימושים ועיבודים במידע בלתי מזוהה, לצורכי תכנון התפעול, התחשבנות בין מפעילים ואספקת שירות כרטיס חכם בתחבורה הציבורית.

3.1.5.3.2. שימוש במידע אישי מזוהה ייעשה רק לשם מתן שירות לנוסע ספציפי ולצורך התגוננות בהליך משפטי.[4]

3.1.5.3.3. **מידע אישי על נתוני מיקום יימחק מיד לאחר ביצוע התחשבנות בין המפעילים**. ככל שהוקם מרכז שירות, יועבר המידע האישי המזהה למרכז השירות בסמוך לאחר הנפקת כרטיס חכם, כך שאצל המפעילים לא יתאפשר לקשר בין מידע אישי מזהה לנתוני מיקום.

3.1.5.3.4. מבלי לגרוע מהאמור, ככל שמרכז השירות יאפשר ללקוח שמעוניין בכך לעיין בתדפיס השימושים שלו בכרטיס בהתאם להוראות הדין, תדפיס כזה יפרט את אזור נסיעה בו בוצע הכרטוס, תעריף ומועד הכרטוס בלבד.

3.1.5.3.5. מובן כי האמור אינו חל על שימושים נוספים הקשורים בכרטיס חכם שאינם קשורים בנסיעה בתחבורה הציבורית. על שימושים אלה יחולו הוראות הדין באופן כללי.

3.1.6. <u>אבטחת מידע</u>

3.1.6.1. כאמור לעיל, מפעילי כרטיס חכם אוספים מידע אישי רגיש אודות הנוסע, בדגש על נתוני המיקום של הנוסע. כמו כן, מפעילי כרטיס חכם נדרשים להתמודד עם סיכונים שונים המתעוררים ביחס להפעלת כרטיס חכם, כגון נגישות עמדות ההנפקה המרוחקות למידע, איסוף הנתונים מעמדות הכרטוס בכלי התחבורה, ביצוע פעולות התחשבנות ואחריות לכרטיסים ועוד.

3.1.6.2. לפי סעיף 17 לחוק על מפעילי כרטיס חכם חלה האחריות לאבטחת המידע במאגר המידע, בהתאם להוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן – **תקנות אבטחת מידע**). ולשם כך עליהם לקיים את ההיבטים המרכזיים הבאים:

3.1.6.2.1. **הפרדת מאגרי מידע אצל המפעיל** - מאגר המידע להפעלת כרטיס חכם כולל מידע בעל רגישות מיוחדת ועל מספר אנשים גדול במיוחד. בשל כך, ולשם מניעת הסיכון כי תהיה אליו גישה בלתי מורשית, יש להפריד את מאגר המידע להפעלת כרטיס חכם ממאגרי מידע אחרים שברשות

[4] בהתאם לפסיקת בית המשפט המחוזי בעת"מ 60829-04-25 **אלקטרה אפיקים בע"מ נ' משרד התחבורה** (נבו 4.12.2025).

מפעילי הכרטיס החכם, כגון מאגר עובדים וכדומה. לעניין זה, הפרדת מאגר המידע יכול שתעשה באופן פיזי או באופן לוגי.

3.1.6.2.2. **הפרדת מידע מזהה מנתונים** - גם במאגר המידע המשמש לפרויקט הכרטיס החכם יש ליצור הפרדות לוגיות או פיזיות בין הנתונים המאפשרים לזהות את הלקוח, לבין הנתונים אודותיו ובכלל זה נתוני הנסיעות שלו.

3.1.6.2.3. **שמירת נתונים על השבב שעל גבי הכרטיס החכם** - בשל החשש מאיסוף לא מורשה של מידע אישי משבב הכרטיס, יש לצמצם את המידע המזהה אודות נוסע הנכלל בשבב רק למידע הנדרש לביצוע החיוב בעמדת הכרטוס, כגון פרופיל הנוסע ותוקף הכרטיס.

3.1.6.2.4. **הגבלת גישה וניטור**

3.1.6.2.4.1. על מפעילי כרטיס חכם לנהל את מאגר המידע האישי באופן שיבטיח שגישה לנתונים הנאספים על ידם תהיה מוגבלת אך ורק לגורמים המורשים לגשת אליהם ואך ורק למטרות לשמן נאסף המידע; במאגר הכולל נתונים שהם מידע בעל רגישות מיוחדת אודות נוסע, יש להגביל את הגישה למאגר רק למקרים בהם גישה זו היא הכרחית לצורך מתן שירות ללקוח, ולצמצם ככל הניתן את מספר הגורמים להם תתאפשר גישה למאגר זה. בנוסף, גישה לנתוני נסיעה בכרטיס מסוים או של נוסע מסוים תתאפשר רק כאשר הנוסע עצמו מבקש לאחזר מידע זה על אודות עצמו, ותוך זיהוי פיזי של הנוסע **באמצעות הכרטיס החכם שבידו**. במקרה של אובדן כרטיס, מוצע כי יונפק לנוסע כרטיס חדש או שהגישה למידע ומסירתו יותנו בהצגת תעודת זהות של הנוסע באופן מתועד שיאפשר בקרה על פעילות העיון במידע וירתיע משימוש לרעה;

3.1.6.2.4.2. על מנת לוודא שלא נעשה שימוש לרעה במידע האישי הנשמר במאגר המידע, יש לעקוב אחר הגישה לנתונים אלה באופן שיאפשר לזהות גישה לא מורשית;

3.1.6.2.5. **נוהל אבטחת מידע** - בהתאם להוראות סעיף 17 ותקנה 4 לתקנות אבטחת מידע, יש לקבוע נוהל אבטחת מידע אשר יחייב את כל העובדים עבור מפעיל הכרטיס החכם או מטעמו.