



הנחית רשם מאגרי מידע 1/2012

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

1. מטרה

1.1. בשנים האחרונות, 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 רשם מאגרי מידע (להלן - **הרשם**) 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. נושא זה נמצא לקראת ההסדרה בחקיקה ראשית. מטרת ההנחיה, בהמשך לטיוטת הנחיה שפורסמה בנושא זה ביוני 2011, לקבוע את הסדרי הביניים עד להסדר ביניים אחר או להשלמה של החקיקה, ובתיאום בין משרד המשפטים, משרד התחבורה והרשם. על רקע חידושים מסוימים בהנחיה שנבעו מהערות הציבור ומחדיון מול משרד התחבורה, סעיף 3.1.3 להנחיה מפורסם להערות בטרם ייכנס לתוקף.

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**).

2.3. במקביל, בכוונת משרד התחבורה להסדיר נושא זה באמצעות חקיקה בצורה מפורטת וברורה יותר¹. עוד מתוכננת הקמת מרכז שירות ארצי שיספק, בין היתר, שירותי סליקה וקיצוץ 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. איסוף מידע על ידי מפעיל כרטיס חכם

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 פיקוחים שביצעה מחלקת רישום ופיקוח ברשות למשפט, טכנולוגיה ומידע (להלן – **"רמו"ט"**) 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 ביחס לכרטיס החכם, כולל מידע 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. בשלב שעל גבי הכרטיס החכם נשמר מידע אישי על הנוסע וכן מידע על נסיעות שבוצעו באמצעות הכרטיס (בהיקף מוגבל כפי יכולות הכרטיס);

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

2.4.5. מהאמור לעיל עולה, כי במסגרת הפעלת כרטיס חכם נאסף מידע במאגר מידע, שחלקו הוא בגדר "מידע רגיש", כהגדרתו בסעיף 7 לחוק.

¹ ראו את הצעת חוק לתיקון פקודת התעבורה (מס' 100) (רישיון מפעיל וכרטיס חכם), התשע"א-2010, ה"ח 541, מיום 18.10.11.

2.5. אבטחת המידע הנאסף על ידי מפעילי כרטיס חכם

- 2.5.1. לפי ההסכם, מחויבים המפעילים לקיום נהלי עבודה ומערכת בקרה על מנת למנוע שימוש לרעה במידע הנאגר 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 ההסכם מפעילי כרטיס חכם נדרשים למנגנוני אבטחה ובקרה.

3. הנחיה

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 היה, כגון תחנת עליה, המאפשרים מעקב פיזי אחר הנוסע (להלן – "נתוני מיקום"). להלן תוצג עמדת רשם מאגרי מידע 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 רגיש כמשמעם בסעיף 7 לחוק, וחלה עליהם החובה לרשום את מאגר המידע המשמש להפעלת כרטיס חכם בפנקס מאגרי המידע לפי 8(ג) לחוק;

3.1.2. מטרת המאגר שתורשם על ידי הרשם, 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. מימוש עקרון המידתיות – אי כבילה בין נסיעה בתחבורה ציבורית לאיסוף מידע (כרטיס אנונימי)

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

שישמרו 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 הרשם 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 להבדק 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.²

3.1.3.5. בהתאם לכך אין להזין לשבב כל פרטים אישיים.

3.1.3.6. בידי הרשם 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.

3.1.4. קבלת הסכמה מהנוסע

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 הרשם כי שככל 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.

² לעניין השימוש במספר תעודת זהות כפגיעה בפרטיות, ראו: בג"צ 6824/07 ד"ר עאדל מנאע נגד רשות המסים, פסקה 37.

3.1.4.5. יודגש כי ככל שמפעיל תחבורה ציבורית מעוניין להקים מועדון לקוחות

או לבצע פעולות שיווקיות אחרות הקשורות באיסוף מידע 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 בהסכם.

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 החיוני לאספקת שירות התחבורה הציבורית ורק לגבי שימוש במידע למטרות הנדרשות במישרין לאספקתו.

3.1.4.7. על ההסכמה שנותן הנוסע להיות הסכמה מדעת, תוך קיום חובת הגילוי לפי סעיף 11 לחוק. בנספח א'1 להנחיה זו מפורט נוסח גילוי מוצע למסירה או העמדה לרשות הנוסעים בעת הנפקת הכרטיס החכם לצורך עמידה בהוראות סעיף 11 לחוק.

3.1.4.8. לצורך קבלת הסכמה מדעת, ובהתאם להוראות סעיף 11(1) לחוק, נדרש 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 והשימוש בו יכולה להינתן רק על ידי מי שהוא האפוטרופוס של הקטין. ככל הניתן, המידע הנשמר במאגר יתייחס לאפוטרופוס של הקטין ולא לקטין עצמו. בנספח א'2 להנחיה זו מפורט נוסח גילוי מוצע לאפוטרופוס של הקטין בעת הנפקת הכרטיס החכם עבורו, לצורך עמידה בהוראות סעיף 11 לחוק. 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 הזכויות לקטין (במקום תאריך הלידה של הקטין, הנדרש היום).³

³ נושא זה ייבחן במסגרת הערות הציבור ובמסגרת השלמה של חקיקת תיקון מספר 100 לפקודת התעבורה.

- 3.1.4.11. בנוסף, ורק על בסיס הבהרה מפורשת כי מדובר בחלק שהינו רשות ולא חובה, ניתן לקבל מספר טלפון של האפוסטרופוס נותן ההסכמה, לצורך יצירת קשר לשם שחזור הכרטיס במקרה אובדן.
- 3.1.4.12. מהאמור נובע גם שלא ניתן להניח כי מי שמעוניין להשתמש בתחבורה הציבורית מעוניין בהכרח להיכלל ב- "מועדון לקוחות" של מפעיל התחבורה הציבורית או כי יעשו עיבודים נוספים הקשורים במידע 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. מטרות השימוש במידע הנאסף באמצעות כרטיס חכם

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

3.1.5.2. שימוש במידע על ידי משרד התחבורה

- 3.1.5.2.1. ככלל, המטרה לשמה נדרש משרד התחבורה לעשות שימוש במידע 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. שימוש במידע על ידי המפעילים

- 3.1.5.3.1. מפעיל כרטיס חכם יכול לבצע שימושים ועיבודים במידע בלתי מזוהה, לצורכי תכנון התפעול, התחשבות בין מפעילים ואספקת שירות כרטיס חכם בתחבורה הציבורית.
- 3.1.5.3.2. שימוש במידע מזוהה ייעשה רק לשם מתן שירות לנוסע ספציפי.
- 3.1.5.3.3. מידע על נתוני מיקום יימחק מיד לאחר ביצוע התחשבות בין המפעילים. ככל שהוקם מרכז שירות, יועבר המידע האישי המזוהה 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 אזור נסיעה בו בוצע הכרטיס, תעריף ומועד הכרטיס 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. אבטחת מידע

3.1.6.1. כאמור לעיל, מפעילי כרטיס חכם אוספים מידע רגיש אודות הנוסע, ובפרט נדרש לשים דגש על כך שנאסף מידע אודות נתוני מיקום 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 הכרטיס בכלי התחבורה, ביצוע פעולות התחשבות ואחריות לכרטיסים ועוד.

3.1.6.2. לפי סעיף 17 לחוק על מפעילי כרטיס חכם חלה האחריות לאבטחת המידע במאגר המידע. 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 רגיש 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 מפעילי הכרטיס החכם, כגון מאגר עובדים וכד'. 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 הכרטיס, 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 באופן שיבטיח שגישה לנתונים הנאספים על

ידם תהיה מוגבלת אך ורק לגורמים המורשים
לגשת אליהם ואך ורק למטרות לשמן נאסף
המידע;

3.1.6.2.4.2. במאגר הכולל נתונים שהם מידע נוסע רגיש, יש
להגביל את הגישה למאגר רק למקרים בהם
גישה זו היא הכרחית לצורך מתן שירות ללקוח,
ולצמצם ככל הניתן את מספר הגורמים שלהם
תתאפשר גישה למאגר זה. בנוסף, גישה לנתוני
נסיעה בכרטיס מסוים או של נוסע מסוים
תתאפשר רק כאשר הנוסע עצמו מבקש לאחזר
מידע זה על אודותיו, 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;

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

3.1.6.2.5. **מנהל מאגר המידע** - מפעילי כרטיס חכם נדרשים למנות
מנהל מאגר מידע, ולציין את שמו ופרטי הקשר שלו בעת
הגשת הבקשה לרישום מאגר מידע לפי סעיף 9(ב) לחוק. נוכח
היקף מאגר המידע ורגישותו יש למנות לתפקיד מנהל המאגר
בעל תפקיד בכיר אצל מפעיל הכרטיס החכם או מנהל הכפוף
ישירות לבעל תפקיד בכיר כאמור;

3.1.6.2.6. **נוהל אבטחת מידע** - לצורך מימוש חובותיהם מכוח סעיף 17
לחוק ומכוח ההסכם, יש לקבוע נוהל אבטחת מידע אשר
יחייב את כל העובדים עבור מפעיל הכרטיס החכם או מטעמו.
על הנוהל להתייחס לנושאים המנויים בנספח ב' להנחיה זו.

3.2. האמור בהנחיה זו ייכנס לתוקף כדלקמן:

3.2.1. **סעיפים 3.1.1, 3.1.2, 3.1.4, 3.1.5.** יכנסו לתוקף ביום 15.03.2012. **ביחס למי שמאגרו**
נרשמו כבר תשונה מטרת המאגר לאמור בסעיפים אלה.

3.2.2. **סעיף 3.1.6** ייכנס לתוקף ביום 15.04.2012, **ועד למועד זה יעבירו המפעילים אל הרשם**
נוהל אבטחת מידע בהתאם לסעיף 3.1.6.2.6.

3.2.3. סעיף 3.1.3 מפורסם בזה להערות מפעילי התחבורה הציבורית והציבור. הוראות אלה יכנסו לתוקף תוך 60 ימים מהמועד שייקבע בתום קבלת ההערות.

נתונים על המידע האישי הנאסף לצורך הנפקת כרטיס חכם בתחבורה ציבורית של חברת _____ (להלן: המפעיל) בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן:

(החוק)

1. מידע מזוהה אודותיך ייאסף וישמר אך ורק לצורך שחזור יתרת הסדרי הנסיעה במקרה של אובדן, גניבה או השחתה של הכרטיס וכן לצורך בדיקת זכאות להנחות והטבות. לא ייאסף וישמר מידע אישי מזהה שאינו נדרש לשם מטרת אלו. הפרטים האישיים שאתה מוסר (שם, דרכים ליצירת קשר ואמצעי תשלום), נדרשים לצורך יצירת קשר איתך בלבד. אתה רשאי למסור את המינימום של הפרטים הנדרש לכך, לפי נוחותך.

2. במידה שאינך מעוניין באפשרות לשחזר את יתרת הסדרי הנסיעה בכרטיס או לקבל זכאות להנחות והטבות, הנך זכאי לרכוש כרטיס חכם אנונימי, אשר אינו שומר מידע אישי בשבב שעל גביו או במאגרי מידע אחרים. כרטיס זה שונה מכרטיס אישי בשני אופנים בלבד:

א. במקרה של אובדן, גניבה או תקלה בכרטיס, לא ניתן יהיה לשחזר את יתרת הסדרי הנסיעה שהייתה טעונה בו עד לאותו מועד.

ב. בהתאם למדיניות ממשלת ישראל, ייתכן שלא תוכל להיות זכאי לחלק מההנחות בתעריפי התחבורה הציבורית.

3. במידה שבחרת לרכוש כרטיס רב קו מזוהה, להלן פירוט ההוראות שיחולו על איסוף ושמירת המידע:

א. פרטים אישיים (שם, פרטי קשר, ואמצעי תשלום) – נשמרים במאגר המידע המרכזי המנוהל בידי המפעיל (להלן – המאגר) לצורך הנפקת כרטיס מזוהה ונגישים לשימוש במרכז השירות של המפעיל רק לצורך מתן שירות ללקוחות כגון במקרה של אובדן, גניבה או השחתה של הכרטיס.

ב. תמונת הלקוח – מודפסת על גבי הכרטיס החכם אך אינה נשמרת במאגר.

ג. מידע על זכאות [דוגמת סטודנט, נכה, פנסיונר] – נאסף ונשמר במאגר לצורך מתן הטבות על פי הפרופיל האישי של הלקוח. המידע יאומת עם הגורם המאשר את הזכאות להנחה (לדוגמא – ביטוח לאומי), והגישה לאימות המידע תעשה רק לצורך מתן ההטבה.

ד. מידע על ביצוע נסיעות הנשמר במאגר המידע – נאסף לצורך התחשבות בין מפעילי התחבורה הציבורית (בקיימם שיתוף בהכנסות מהסדרי נסיעה משותפים) וחישוב יתרת הכרטיס. מידע הנסיעות המזוהה יעבור הליך של מחיקת נתוני בעל הכרטיס (אנונימיזציה) לאחר תהליך ההתחשבות. הגישה למידע תהיה ללא נתונים מזהים, ככל הניתן.

4. עם הנפקת כרטיס רב קו מזוהה הנך נותן את הסכמתך לכך שהמפעיל:

א. יאסוף, יבדוק ויאמת את המידע שנמסר בטפסי הרישום ומסמכי הזכאות לשם הנפקת הכרטיס, בירור זכאותך להנחה או להטבה והיקף זכאותך;

ב. ישמור מידע אודות הנסיעות שלך, לצורך שחזור כרטיס שאבד, נגנב או הושחת, ולצורך שירות לקוחות. המידע יישמר באופן שלא יעשה בו שימוש אלא למטרה זו. הגישה

⁴ הנוסח הוכן על רקע ההנחיה וכהשלמה לה.

למידע תוגבל למי שרשאים לתת שירות כאמור, והוא יימסר לך רק לאחר שזוהית באמצעות כרטיס חכם או אמצעי אחר.

ג. יעביר מידע כמפורט בסעיף 1, למרכז שירות אשר פעולתו מוסדרת על ידי משרד התחבורה לצורך ביצוע כל אחת מהפעולות האמורות לעיל.

ד. יעביר מידע כמפורט בסעיף 1 למשרד התחבורה לצורך מימוש תפקידיו. ככלל, מידע זה יהיה אנונימי לצרכים סטטיסטיים בלבד, אולם יתכן כי במסגרת פיקוח אצל המפעילים ובירור תלונות שהוגשו נגדם, יידרש משרד התחבורה למידע מזוהה לצורך מטרות אלה.

5. החוק מעניק לכל לקוח **זכות לעיין במידע המוחזק עליו במאגר המידע** שברשות המפעיל. מימוש הזכות ייעשה בתיאום עם משרד התחבורה.

נספח א'2 – נוסח מוצע לדף גילוי נאות של מפעילי כרטיס חכם לקבלת הסכמה מדעת

מהאפוטרופוס החוקי של קטין לאיסוף מידע אודות הקטין

נתונים על המידע האישי הנאסף לצורך הנפקת כרטיס חכם לקטין בתחבורה ציבורית של חברת

_____ (להלן: המפעיל) בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן:

החוק)

1. מידע על קטין ייאסף וישמר אך ורק לצורך בקרת זכאות ולצורך שחזור יתרת הסדרי הנסיעה במקרה של אובדן, גניבה או השחתה של הכרטיס. לא ייאסף וישמר מידע אישי מזהה שאינו נדרש לשם מטרות אלו. הפרטים האישיים שאתה מוסר (שם, דרכים ליצירת קשר ואמצעי תשלום), נדרשים לצורך יצירת קשר איתך בלבד. אתה רשאי למסור את המינימום של הפרטים הנדרש לכך, לפי נוחותך.

2. המידע אותו המפעיל רשאי לאסוף לצורך הנפקת כרטיס מזהה הוא המידע הבא בלבד: מספר תעודת הזהות של האפוטרופוס נותן ההסכמה, שם הקטין, ומועד פקיעת הזכאות, וכן מידע הנדרש ליצירת קשר ושחזור הכרטיס.

3. להלן פירוט ההוראות שייחולו על איסוף ושמירת המידע:

א. פרטים אישיים אודות האפוטרופוס (שם, פרטי קשר ואמצעי תשלום) ושם הקטין – נשמרים במאגר המידע המנוהל בידי המפעיל (להלן – המאגר) ונגישים לשימוש במרכז השירות של המפעיל רק לצורך מתן שירות ללקוחות כגון במקרה של אובדן, גניבה או השחתה של הכרטיס.

ב. תמונת הקטין – מודפסת על גבי הכרטיס החכם ולא נשמרת במאגר.

ג. מידע על ביצוע נסיעות – נאסף לצורך התחשבות בין מפעילים וחשוב יתרת הכרטיס. מידע הנסיעות המזוהה יעבור הליך של מחיקת נתוני בעל הכרטיס (אנונימיזציה) לאחר תהליך ההתחשבות. הגישה למידע תהיה ללא נתונים מזהים, ככל הניתן.

4. עם הנפקת כרטיס רב קו מזהה הנך נותן את הסכמתך לכך שהמפעיל:

א. יאסוף, יבדוק ויאמת את המידע שנמסר אודות הקטין בטפסי הרישום לשם הנפקת הכרטיס.

ב. ישמור מידע אודות נסיעות, לצורך שחזור כרטיס שאבד, נגב או הושחת, ולצורך מתן שירות לקוחות בהקשר זה. המידע יישמר באופן שלא ייעשה בו שימוש אלא למטרה זו. הגישה למידע תוגבל למי שרשאים לתת שירות כאמור, והוא ימסר לך רק לאחר זיהוי הלקוח באמצעות כרטיס חכם או אמצעי אחר.

ג. יעביר מידע, שנדרש על מנת לשחזר את יתרת הסדרי הנסיעה (כאמור בסעיף 1), למרכז שירות אשר פעולתו מוסדרת על ידי משרד התחבורה.

ד. יעביר מידע, שנדרש על ידי משרד התחבורה לצורך מימוש תפקידיו. ככלל, מידע זה יהיה אנונימי לצרכים סטטיסטיים בלבד, אולם יתכן כי במסגרת פיקוח אצל המפעילים ובירור תלונות שהוגשו נגדם, יידרש משרד התחבורה למידע מזהה לצורך מטרות אלה.

5. החוק מעניק לכל לקוח זכות לעיין במידע המוחזק עליו במאגר המידע שברשות המפעיל. מימוש הזכות ייעשה בתיאום עם משרד התחבורה.

נספח ב' – רשימת נושאים להתייחסות בנוהל אבטחת מידע אצל מפעילי כרטיס חכם

1. מיפוי רכיבי המערכות, מבנה הרשת שבה פועל המאגר וכן מיפוי של שדות המידע הנשמר במאגר המידע ;
2. הערכת הסיכונים המרכזיים לפגיעה בנושא המידע (הנוסע), עקב חשיפתו או שימוש בו שלא כדין, או ללא הרשאה כדין, ואופן ההתמודדות איתם ;
3. אופן קביעת הרשאות גישה למידע במאגר ;
4. הוראות לעניין עיבוד המידע באמצעות מיקור חוץ ;
5. הוראות למורשי הגישה למאגר המידע לצורך שמירה על אבטחת המידע במאגר בעת השימוש בו ;
6. הוראות בעניין האבטחה הפיזית והסביבתית של מתקני המאגר ;
7. אופן הבקרה על השימוש במאגר המידע, ובכלל זה רישום של הגישה למערכות המחשוב של המאגר ;
8. הוראות לעניין גישת אנשי הפיתוח לנתונים במאגר לצרכי פיתוח ובדיקות ;
9. הוראות לעניין אבטחת מערכות התקשורת אל מערכות המאגר וממנו ;
10. הוראות לעניין ביצוע ביקורות תקופתיות כדי לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ;
11. אמצעים לשמירה על עדכניות נוהל האבטחה, ומועדים או אירועים בגינם תידרש בחינתו מחדש, כגון עריכת שינויים מהותיים במערכת או עקב הביקורת התקופתית.
12. אופן ביצוע אנונימיזציה (הסרת מידע מזהה אודות נושא המידע) במאגר המידע.

למידע נוסף על הנושאים שפורטו לעיל ניתן לעיין בנייר עמדה בנושא אבטחת מידע לצורך חוק הגנת הפרטיות שפרסמה רמו"ט, בכתובת : www.justice.gov.il/NR/rdonlyres/8D081CC2-225B-4269-95F7-BF6860654DA4/18194/tyutat_takanot_avtachat_meida_100112.pdf

מידע לגבי ההנחיה

1. מס' ההנחיה: 1/2012
2. נושא ההנחיה: תחולת הוראות חוק הגנת הפרטיות על מאגרי מידע של מפעילי כרטיס חכם בתחבורה ציבורית
3. תאריך פרסום: 27.2.12
4. בתוקף מתאריך: בהתאם לקבוע בסעיף 3.2 להנחיה
5. חוקים שאוזכרו:
 - א. חוק הגנת הפרטיות, התשמ"א-1981.
 - ב. תקנות התעבורה, התשכ"א-1961.
6. פסקי דין שאוזכרו: בג"צ 6824/07 ד"ר עאדל מנאע נגד רשות המסים;
7. מאמרים שאוזכרו: אין.
8. הנחיות היועץ המשפטי לממשלה שאוזכרו: אין.
9. הנחיות רשם מאגרי מידע שאוזכרו: אין.
10. מילות מפתח: אבטחת מידע, אנונימיות, גילוי, כרטיס חכם, מאגר מידע, מדיניות פרטיות, מטרות שימוש במידע, מידע רגיש, מנהל מאגר, נוסע, נתוני מיקום, רישום, שימוש במידע, שקיפות, תחבורה ציבורית.
11. עדכונים

גרסה	פרטים	תאריך