התנועה לזכויות דיגיטליות
Digital Rights Movement

תאריך: 01/06/2011

לכבוד הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים
באמצעות דוא"ל ILITA@justice.gov.il

הנדון: הערות התנועה לזכויות דיגיטליות על טיוטת הנחיות רמו"ט בנוגע למאגרי מידע של מפעילי כרטיס חכם בתחבורה הציבורית

אנו מברכים על פרסום טיוטת הנחיות רשם מאגרי המידע בנוגע למאגרי מידע של מפעילי כרטיס חכם בתחבורה הציבורית (כרטיסי הרב-קו), ורואים בפרסום טיוטת ההנחיות צעד ראשון לפתיחת השיח הציבורי בנושא. עם זאת, בהתחשב בבעיות הפרטיות שהתגלו לאחרונה בנושא השימוש בכרטיסים חכמים בתחבורה הציבורית, הגילוי כי הכרטיס מאפשר לחברות התחבורה הציבורית לעקוב אחר נוסעיהן, והמידע כי רשויות אכיפת החוק עשו שימוש במאגר המידע ללא צו שיפוטי הולם, אנו מקווים כי ההנחיות לא יהפכו לאות מתה.

לדעתנו, בעיות הפרטיות נובעות מכך שעקרונות ה-Privacy by design לא נשקלו בעת עיצוב ותכנון המערכת. עתה, עם כוונת משרד התחבורה להסדיר את הנושא בדרך של חקיקה ראשית והתקנת תקנות מכוחה, נראה שהנושא זוכה לבדיקה יסודית, והנחיות רשם מאגרי המידע הינן פן אחד במסגרת ההסדרה (כאמור בסעיף 2.3 בטיוטת ההנחיות).

נבקש לנצל במה זאת כדי להעיר מספר הערות לגבי עיקרון ה-Privacy by design (להלן, PbD), שלטעמנו נדרש להיות מיושם בפריסת מערכת הכרטוס החכם בתחבורה הציבורית. על כן, במסמך זה נציג התייחסות כוללת של התנועה לזכויות דיגיטליות לנושא ההסדרה, ובמסגרתה התייחסות פרטנית לטיוטת ההנחיות. נסביר כיצד לטעמנו יש לשלב את עקרונות הפרטיות באפיון ובאופן פעולת המערכת, וכיצד לטעמנו יש לגזור מעקרונות אלו את הנחיות רשם מאגרי המידע. בנוסף, נתייחס להטמעת עקרונות הפרטיות בהצעת החוק לתיקון פקודת התעבורה (מס' 100) (רישיון מפעיל וכרטיס חכם), התשע"א-2010, הנדונה בימים אלו בוועדה המשותפת לוועדת הכלכלה ולוועדת הכנסת[1].

עיצוב המערכת בהתאם לעקרונות הפרטיות

התנועה לזכויות דיגיטליות רואה את עיקרון ה-PbD כעיקרון מנחה והכרחי לצורך תכנון מערכת הכרטוס החכם ככלל, ומאגרי המידע של מפעילי כרטיסים חכמים בפרט, בדרך שלא תפגע בפרטיותם של הנוסעים, צרכני התחבורה הציבורית.

מר יהושע שופמן, יו"ר המועצה הציבורית להגנת הפרטיות, הציג את עיקרון ה-PbD בדיון שנערך לאחרונה על הצעת החוק:

> כדי לענות על בעיות הפרטיות ובלי לפגוע בנוסע הדבר שצריך לעשות הוא לא כל כך לקבוע הוראות נורמטיביות על איסור העברת מידע ועבירות פליליות על שימוש לרעה, אלא לעצב מראש את המערכת בצורה שמגינה על הפרטיות, מה שנודע בעולם כ-privacy by design.

מהפרוטוקול עולה כי גם משרד התחבורה תומך בכך, לפחות באופן הצהרתי:

> במשרד התחבורה אנחנו רואים בשמירה על הפרטיות ערך מאוד חשוב, בכלל בקיומה של המערכת הזאת. לדעתי, אף אחד לא השתמש בה, אלא אם כן היא תשמור על הפרטיות. לכן זה אינטרס משותף שלנו בכלל בקיום הכרטיס. נודע לנו רק לא מזמן על דרך העבודה של privacy by design, ומאז שנודעה לנו המתודולוגיה של העבודה אנחנו מנסים ללכת בדרכה, כולל לברר בעולם איך מתמודדים עם העניין הזה. נכנסנו ל-mode עבודה מאוד צמוד והדוק ברמה הפרטנית מול החברים במשרד המשפטים בדיוק בשביל לפתור את כל הבעיות האלה.

1 פרוטוקול מס' 1 מישיבת הוועדה המשותפת לוועדת הכלכלה ולוועדת הכנסת מיום 21/02/2011.

חברי הכנסת שהשתתפו בדיון התייחסו גם הם בדאגה לפגיעה האפשרית בפרטיות הנוסעים. מכאן נראה כי קיים קונצנזוס – מוצהר לפחות – על חשיבותו של עיקרון ה-PbD בתכנון המערכת וההתייחסות למידע הנשמר בה.

משרד התחבורה בחר בטכנולוגיה של Calypso להקמת מערכת הכרטוס החכם בתחבורה הציבורית. טכנולוגיה זאת ניטרלית מבחינת פרטיות, ומאפשרת תכנון והפעלת מערכות חיוב וסליקה תחת כל דרישות או הנחיות פרטיות נתונות[2]:

> Calypso specifications only deal with the contactless transaction between a terminal and a portable object, they don't include information about the back-office management system and the collection of transaction data.
>
> [...]
>
> In fact, Calypso is privacy-neutral, meaning that its secure e-transaction uniquely requires systems that use it to comply with the recommended privacy guidelines currently in use. It is thereafter the operators' responsibility to maximize protection of personal information, by limiting them to the appropriate time period and increasing confidence among users by explaining how private information is protected.

דהיינו, הטכנולוגיה מותירה בידי המפעילים (ובידי הרגולטור) את האפשרות לקבוע את רמת ההגנה על פרטיות המשתמשים במערכת המותקנת.

לכן, בטרם נעבור להתייחסותנו המפורטת לטיוטת ההנחיות, **נבקש להמליץ כי הדרישה לאפיון ולתכנון המערכת עפ"י עקרון ה-PbD תקבע במסגרת חקיקה ראשית. נמליץ כי התקנות המסדירות את הנושא ינוסחו בהתאם לעיקרון זה, והדבר יקבע ויירשם מפורשות בתיקון המוצע לסעיף 71(ב) של פקודת התעבורה.**

לטעמנו, הסדרת עיקרון ה-PbD במסגרת החקיקה הראשית הכרחית למניעת כרסום עתידי בדרישות הפרטיות. מניסיון העבר, אנו צופים שני תהליכים שעלולים להביא לכך. ראשית, בהתאם להצהרת משרד התחבורה, המערכת הקיימת לא תוכננה עפ"י עיקרון ה-PbD, ולכן צפוי כי התאמת המערכת לדרישות הפרטיות תדרוש השקעת משאבים. המפעילים ומשרד התחבורה עלולים לטעון כי כל שינוי בדרך פעולת המערכת הקיימת ייקר את המעבר, וכך ייווצר לחץ כנגד הטמעת עקרונות הפרטיות במערכת. בנקודה זאת ראוי לחזור ולהדגיש כי הטכנולוגיה של Calypso גמישה דיה כדי לאפשר הטמעה של כל רמת פרטיות מבוקשת.

שנית, אנו חוששים שבפועל עיקרון ה-Privacy by design יפנה את מקומו לעיקרון ה-Police usage by design, כפי שנוכחנו לראות בתהליכים להקמת המאגר הביומטרי[3]. בנקודה זאת ראוי להאיר נקודה מעט טכנית, והיא שהטכנולוגיה שנבחרה חשופה להתקפות מסוג man-in-the-middle, ולכן ראיות איכון המופקות באמצעותה ניתנות לזיוף[4].

---

2 "Calypso and Users Privacy", מתוך Calypso Handbook, מצ"ב.

3 ניצן סדן, איתן: "המאגר הביומטרי יופעל בניגוד לחוק", ynet, 27/02/2011.
עירא אברמוב, פיילוט המאגר הביומטרי – נחטף?, אסכולת הכורסא, 10/03/2011.
טלילה נשר, בלעדי: למשטרה תהיה גישה למאגר הביומטרי, גל"צ, 06/04/2011.
דן חי, האח הגדול כבר לא מוצפן, TheMarkerIT, 26/05/2011.

4 בהתקפות man-in-the-middle (או Relay attacks), ראובן מתחזה לשמעון באמצעות הצבת מכשיר ממסר RFID ליד ארנקו של שמעון ובאמצעות כרטיס ממסר המוחזק אצלו, שניהם מתקשרים אחד עם השני במרוחק. ראובן מגיע לשער (תחנת זיהוי), וכרטיס הממסר שבידו קולט בקשת הזדהות מהשער. כרטיס הממסר מעביר את הבקשה למכשיר הממסר המוצב ליד שמעון. הכרטיס של שמעון עונה על בקשת ההזדהות בפני מכשיר הממסר, כי הוא קולט בקשת הזדהות לגיטימית של שער אמתי, ומכשיר הממסר מעביר את התשובה לכרטיס הממסר שבידי ראובן. כך ראובן עונה על הבקשה כאילו הוא שמעון, והכרטיס של שמעון ומערכת הכרטוס, שניהם "יודעים" ששמעון עבר בתחנת הזיהוי, ולא ראובן.
ראה Ross Anderson, RFID and Middleman, וכן Bruce Schneier, RFID Cards and Man-in-the-Middle Attacks, וכן Ziv Kfir & Avishai Wool, Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems.
ראוי לציין כי התחזות כזאת דורשת כיום חומרה ייעודית, אך המומחים צופים כי בעתיד טלפונים NFC יאפשרו התקפות מהסוג המתואר ע"י תוכנה מתאימה.

התייחסות פרטנית לעקרונות המערכת ולטיוטת ההנחיות

התייחסותנו תהיה בשתי רמות – כיצד יש לממש את עקרונות הפרטיות במסגרת אפיון ותכנון המערכת ומאגרי המידע העתידיים, וכיצד ניתן להתאים (חלקית) את המערכת הקיימת לעקרונות אלו באמצעות הנחיות רשם מאגרי המידע.

המידע הנשמר בזיכרון הכרטיס החכם

כמו כל כרטיס, גם כרטיס חכמים עלולים ללכת לאיבוד. בכדי שפרטיות המשתמשים תשמר גם במקרה אבדן או גנבה, אין לשמור בכרטיס מידע רגיש או אישי. לטעמנו אין צורך שהכרטיס יכיל מידע אישי מעבר לסוג הכרטיס ולמזהה נומרי של בעליו (במקרה של כרטיס מזוהה). אמנם Calypso מאפשרים לשמור את המידע באופן מוצפן, אך כל מסוף מסוגל לקרוא את המידע השמור על הכרטיס, ובכל מקרה, הצפנות אלו אינן עמידות בפני התקפות חומרה מתקדמות[5].

טיוטת ההנחיות לא מתייחסת למידע הנשמר בזיכרון הכרטיס עצמו. אנו ממליצים כי לצורך אבטחת המידע, הרשם ינחה בסעיף 2.6.4 שלא יישמר כל מידע דמוגרפי מעבר למזהה נומרי של הנוסע, וכן להימנע מאיסוף מידע בדבר הנסיעות האחרונות של הנוסע (למעט הרשומות האחרונות של מעבר בתחנות זיהוי, לצורך חיוב בכניסה, ביציאה או ביקורת, בהתאם לתקן Calypso).

כרטיסים אנונימיים כארנקים אלקטרוניים

בכל הנוגע לארכיטקטורה הטכנולוגית של הכרטיס, אנו מציעים כי הרשות תמליץ למפעילי הכרטיס החכמים לעבוד במודל בו הכרטיס החכם משמש כארנק אלקטרוני, כלומר במעבר של האדם בשער מתבצעת עסקה אלקטרונית בין הכרטיס החכם ומפעיל התחבורה הציבורית, ותעריף הנסיעה נגרע מהסכום שהוטען בכרטיס. הדבר דומה לשימוש בכסף מזומן, אשר מאפשר את התחבורה הציבורית, ובעולם מפעילים רבים משתמשים במודל מסוג זה עבור כרטיסיהם האנונימיים. בהתחשב באמינות הקריפטוגרפית הגבוהה יחסית של ארנקים אלקטרוניים[6], ובהתחשב בכך שעלות זיוף כרטיסים מסוג זה גבוהה בהרבה מהתועלת שניתן להשיג מזיופם, הרי שקיימת עדיפות למודל בו המידע מאוחסן על הכרטיס החכם ולא על שרת מרכזי.

הנפקת כרטיסים אנונימיים כברירת מחדל

לכרטיסים מזוהים שני יתרונות על הכרטיסים האנונימיים. היתרון הראשון הוא האפשרות, במקרה של גנבה או אבדן הכרטיס, להנפיק לנוסע כרטיס חדש עם היתרה הכספית הלא-מנוצלת. היתרון השני הוא הנפקת כרטיסי נסיעה אישיים מסוג "חופשי חודשי". אך לכרטיסים מזוהים גם חסרונות, והנפקה של כרטיס מזוהה דורשת המתנה לפקיד אנושי, ומהווה פרוצדורה מסובכת יחסית בהשוואה לקניית כרטיס חכם במכונה אוטומטית לממכר כרטיסים.

בבריטניה מופעלת בהצלחה מערכת כרטוס חכם הקרויה "Oyster", מערכת הנמצאת בשימוש מפעילי תחבורה ציבורית באזור לונדון רבתי. מכונות הממכר בלונדון מנפקות כרטיסי Oyster אנונימיים בלבד, וזאת ברירת המחדל לקניית הכרטיס. לאחר הקנייה, הנוסע יכול לרשום את כרטיסו[7], וכך לבטח את הכרטיס במקרה של אבדן או גניבה.

לטעמנו, ראוי כי גם אצלנו ברירת המחדל תהא הנפקת כרטיס אנונימי, שלאחר הנפקתו הנוסע רשאי לבצע את רישומו לצורך ביטוח הסכום הלא-מנוצל בכרטיס. כהערת אגב נציין כי רישום הכרטיס אינו דורש עקרונית הזדהות מלאה, אלא רק בחירת קוד או שאלת ביטחון לשם ביטול תוקף כרטיס אבוד והעברת היתרה הלא-מנוצלת לכרטיס החדש.

טיוטת ההנחיות כוללת התייחסות להנפקת כרטיסים אנונימיים בסעיף 2.7.2. אנו ממליצים כי הנחיה בנוגע לפרוצדורת רישום כרטיסים אנונימיים בדומה לדגם הלונדוני של כרטיסי ה-Oyster תתווסף בסעיף זה.

---

5 להסברים על Invasive Physical Attacks, ראה http://cl.cam.ac.uk/~mgk25/sc99-tamper-slides.pdf.

6 ארנקים אלקטרוניים משתמשים בחתימות אלקטרוניות כדי להבטיח אותנטיות של מבצעי העסקה ואישור על ביצועה.

7 לפרטים אודות הליך רישום כרטיסי ה-Oyster, ראה http://ukbytheway.co.uk/oyster-card-registration.

איסור אפליית מחירים בין כרטיסים אנונימיים וכרטיסים מזוהים

לטעמנו יש לחדד את האיסור על אפליית מחירים הנרמז בסעיף 2.7.2. נמליץ כי יירשם בהנחיות במפורש כי אם קיימת הנחה כללית – למשל הנחת כמות על הטענת סכום כסף גדול – אזי הנחה זהה תינתן בין אם הכרטיס אנונימי ובין אם מזוהה. לעניין זה, התעריף היחיד שיש הצדקה כלכלית לשונות הוא עלות ההנפקה, כי הנפקת כרטיס מזוהה דורשת יותר משאבים בהשוואה להנפקה ממוכנת של כרטיס אנונימי.

אנו ממליצים כי ייאסר על מפעילים להתנות מתן הנחה בפגיעה באנונימיות או בפרטיות של הנוסעים, בהתחשב בכך שאין צורך ממשי בפגיעה זו כדי לתת את ההנחה. כלומר תיאסר פגיעה במחזיקי הכרטיסים האנונימיים לעומת מחזיקי הכרטיסים המזוהים.

כרטיסים אנונימיים ייעודיים

בהתאם לסעיף 2.4.1 לטיוטת ההנחיות, נוסע המבקש לקנות כרטיס חכם הכולל הנחות ייעודיות, נדרש לקנות כרטיס מזוהה ולתת פרטים מזהים שונים, פרטי מידע הנשמרים למשך 7 שנים אצל המפעיל. בהתאם לנוהל, בכדי לקבל הנחה ייעודית על המבקש להוכיח את זכאותו באמצעות הצגת תעודת זכאות מתאימה: תעודת תלמיד לתלמידים ולנוער, תעודת חוגר או קצין לחיילים, תעודת סטודנט לסטודנטים, תעודת אזרח ותיק לאזרחים ותיקים, וכן הלאה. הליך זיהוי ואשרור ההנחה מתבצע במועד הנפקת כרטיס חכם אישי ומזוהה.

לטעמנו, אין סיבה שלא יונפקו כרטיסים אנונימיים גם לזכאי הנחות, וכי דין כרטיסים אנונימיים ייעודיים כדין כרטיסיות ייעודיות. כיום מונפקות לזכאים כרטיסיות אוטובוס הכוללות הנחה (למשל כרטיסיות נוער). בעת השימוש בכרטיסייה, הנוסע נדרש להציג את תעודת הזכאות המתאימה להנחה המגולמת בה. לטעמנו, באותו האופן ניתן להשתמש בכרטיס אנונימי ייעודי: בעת השימוש בכרטיס, הנוסע יידרש להציג את תעודת הזכאות המתאימה להנחה המגולמת בו. כך, לא תדרש הנפקת כרטיסים מזוהים לשם ניצול ההנחה הייעודית.

להבדיל מהכרטיסים המזוהים, כרטיסים אנונימיים אלו ניתנים להעברה במסגרת קבוצת הזכאים. כך, כפי שתלמידי בית הספר משאילים אחד לשני כרטיסיות נוער, כך יוכלו להשאיל אחד לשני כרטיסי נסיעה ייעודיים לנוער. כך, כפי שתלמידי בית הספר נוהגים "לנקב" אחד על השני (כלומר תלמיד משלם על חברו), לא תהיה מניעה עקרונית שהם יוכלו לשלם אחד על השני באמצעות הכרטיסים הייעודיים לנוער. דבר זה אינו אפשרי אם הנחות תלמידים יינתנו אך ורק ע"י כרטיסים מזוהים שאינם ניתנים להעברה.

למעשה, היתרון היחיד לכרטיס מזוהה הוא הסרת ההכרח להציג את תעודת הזכאות בכל עת שנעשה שימוש בכרטיס. כלומר הוכחת הזכאות מתבצעת פעם אחת ויחידה במועד הנפקת הכרטיס המזוהה.

ראוי לציין כי חוק האזרחים הותיקים, תש"ן-1989, דורש לכאורה הנפקת כרטיסים אנונימיים ייעודיים. סעיף 10(א) לחוק קובע כי הנחה לאזרחים ותיקים תינתן על כל סוגי הכרטיסים הקיימים, וכרטיס אנונימי הוא אחד מסוגי הכרטיסים הקיימים בתחבורה הציבורית:

> **אזרח ותיק זכאי להנחה בשיעור של 50% מדמי הנסיעה בתחבורה הציבורית, הן העירונית והן הבין-עירונית, והיא תינתן על כל סוגי הכרטיסים הקיימים בתחבורה הציבורית.**

טיוטת ההנחיות אינה מתייחסת לאפשרות הנפקת כרטיסים אנונימיים ייעודיים, אך לטעמנו ראוי כי בעת התקנת התקנות המחוקק יתייחס לאפשרות זאת.

שמירת מאפייני הנחה בכרטיסים מזוהים

כאמור לעיל, אין כל מניעה עקרונית או טכנולוגית לתת הנחות ייעודיות בכרטיסים אנונימיים. היתרון של כרטיסים מזוהים (בהקשר זה) הוא שהמבקש נדרש להוכיח את זכאותו רק בעת הנפקת הכרטיס המזוהה, ולא בכל פעם שנעשה שימוש בכרטיס. כרטיסים מזוהים הינם מחויבי המציאות רק עבור כרטיסי נסיעה אישיים מסוג "חופשי חודשי", כרטיסים המאפשרים לנוסע נסיעה חופשית למשך פרק זמן נתון.

עבור קבוצות נוסעים אלו, ובהתאם לנאמר בסעיפים 2.4.1-2.4.2 לטיוטת ההנחיות, נאספים ונשמרים פרטי מידע דמוגרפי אודות הנוסע המבקש להפיק כרטיס מזוהה. כאמור, על המבקש להוכיח את זהותו ואת זכאותו במקרה הצורך. איננו מבינים מדוע לאחר המפעיל נדרש לשמור את המידע הדמוגרפי על

הנוסע. לטעמנו אין כל סיבה כי ישמר כל מידע דמוגרפי, מעבר לקוד ההנחה לה הנוסע זכאי.

הערה דומה העלו חברי הכנסת שדנו בהצעת חוק לתיקון פקודת התעבורה לעיל, וגם הם תהו מדוע נשמרים ללא צורך פרטים אישיים של הנוסע:

אתי בנדלר: **נניח שיש הנחות למקבלי גמלאות של המוסד לביטוח לאומי. אז הפרט הזה צריך להיות במאגר המידע, שהוא מקבל גמלת נכות.**

ישראל אייכלר: למה זה צריך להיות?

אתי בנדלר: כדי שהוא יכול לקבל הנחה.

ישראל אייכלר: **אז ברגע שהוא מקבל את הגמלה יש לו מספר 1, וזהו.**

יערה למברגר: זה מה שיש, יש קוד.

ישראל אייכלר: לא שהמפעילים יוכלו לבדוק--

היו"ר יריב לוין: הוא לא צריך לבדוק, **הוא יודע אוטומטית ברגע שיש מספר 1 שהוא נמצא בקטגוריה של זכאים להנחה.**

ישראל אייכלר: בסדר, כי הנוסע רוצה הנחה, **אבל אני לא רוצה – גם אם אני נכה – שתהיה לכם אפשרות לבדוק ממה אני נכה ואיזה אישורים יש לי.**

טיוטת הנחיות רשם מאגרי המידע מתייחסת למאגרי המידע הקיימים. לכן נמליץ כי עם התקנת התקנות יוסרו מהמאגרים פרטי המידע שאינם נדרשים לצורך הפעלת המערכת.

איסוף מידע על הנסיעות לצורך "שיפור השירות"

בהתאם לאמור בסעיף 2.4.3 לטיוטת ההנחיות, נאספים "נתוני השימוש בכרטיס כגון מספר הקו, מספר כלי התחבורה בו בוצעה הנסיעה, תחנת העלייה על אמצעי התחבורה ושעת העלייה עליו". ברור לכל בר-דעת כי איסוף נתונים אגרסיבי כזה גורם לפגיעה חמורה ומיותרת בפרטיות הנוסעים, ואינו נדרש לשום צורך מעשי. (גם שימושו לצרכים משטרתיים מוגבל, עקב האפשרות לזייף ראיות האיכון, כאמור בהערה 4 לעיל, ובכל מקרה לא ייתכן כי מאגר מידע רגיש יתוכנן בצורה פגומה רק בכדי לתת למשטרה כלי מעקב חדש).

לטעמנו, אין משמעות לכך שאדם אלמוני או אדם פלוני, "בבוקר קם, ובקו 5 נוסע אל הים", אלא רק למספר הנוסעים שקמו בבוקר ונסעו אל הים. כלומר, די בכך שהמפעיל ישמור מידע בלתי מזוהה לגבי כמות הנוסעים העולים וכמות הנוסעים היורדים בכל תחנה. מידע סטטיסטי מסוג זה יכול לשרת את אותה מטרה תוך פגיעה פחותה בפרטיות האזרחים. לכן, נדרש הליך של דיסוציאציה (data dissociation), בו מופרדים נתוני הנוסע מנתוני הנסיעה. הליך זה חייב להיות מוטמע בדרך הפעולה המוגדרת של המערכת, וחובה על התקנות לקבוע כי מידע כה רגיש לא ייאסף (למעט בצו בית משפט). לעומת זאת, מידע סטטיסטי על הנסיעות ללא שיוך לנוסעים ספציפיים אינו פוגע בפרטיות ואין בעיה כי ייאסף לצורך שיפור השירות או לכל מטרה אחרת.

ייתכן כי מערכת הכרטוס החכם דורשת שמירת מידע על הנסיעה האחרונה של הנוסע (למשל לשם ביקורת כרטיסים), אך בבירור אין צורך לשמור את המידע יותר מאשר יום-יומיים, ובוודאות אין כל סיבה או צורך לשמור את המידע 7 שנים (כאמור בנספח א' לטיוטת התקנות). אנו ממליצים כי הרשם ידרוש מהמפעלים לקבוע מדיניות שימור מידע (Data retention policy) שבהתאם לה המידע הרגיש לא יישמר מעבר לזמן המינימלי הנדרש לשם פעולתה התקינה של המערכת (למעט בצו בית משפט). לעומת זאת, מידע סטטיסטי על הנסיעות ללא שיוך לנוסעים ספציפיים יכול להישמר לעולמי-עד ללא הגבלה.

בינתיים, בבחינת "אצבע בסכר", נמליץ כי טיוטת ההנחיות יחייבו את הפרדת מאגרי המידע של הנוסעים ושל נסיעותיהם, וכי תיאסר הצלבת נתונים ללא צו מתאים.

מטיוטת ההנחיות ניתן להבין כי גם כרטיסים אנונימיים אוספים מידע מזהה על אדם, דבר שיכול לפגוע בפרטיותו. איסוף מידע כי נוסע בעל כרטיס מסוים עולה בתחנת אוטובוס ונוסע כל יום בשעות מסוימות ליעד מסוים הוא מידע אישי מזהה לכל דבר, גם אם שמו אינו צמוד למידע זה. לכן יש לאפשר לנוסע לקבל כרטיס אנונימי בו המידע על אודות נסיעותיו אינו נשמר כלל. הדירקטיבה האירופית מכירה בזכות דומה, והיא קובעת למשל כי לבעלי מידע הזכות למנוע משירותי אינטרנט לעקוב אחריהם.

לטעמנו, מן הראוי לקבוע כי ברירת המחדל תהיה שהכרטיס לא יאסוף מידע, אלא אם התקבלה הסכמה מפורשת מהנוסע (בדומה לסעיף 3.1.4 לטיוטת ההנחיות). שימוש זה מאמץ את ההסכמה הדרושה לצורך פגיעה בפרטיות, והוא האיזון הראוי. בכל הנוגע לשימוש של כרטיסים חכמים על ידי קטינים, ראוי כי הורים יקבלו ידיעה על מדיניות הפרטיות של הכרטיסים החכמים ויסכימו לאיסוף המידע. בשאלת חוקיות איסוף מידע על קטינים, ראוי לטעמנו כי תתבקש גם התייחסות המועצה לשלום הילד לנושא. חשוב להבהיר כי איסוף מידע על נתוני נסיעה של קטינים, לרבות שעות יציאתם מבית הספר ומקום מגוריהם המקורב, עשוי לגרום לנזק רב יותר מהתועלת שתופק מאיסוף המידע. על-כן, נמליץ כי בטיוטת ההנחיות תידרש גם הסכמה מדעת לשם איסוף מידע על הנסיעות.

סיכום

אנו רואים בטיוטת ההנחיות צעד בכיוון הנכון. יחד עם זאת, אנו רואים בטיוטה צעד אחד במסגרת תהליך ארוך של הסדרת מערכת הכרטוס החכם במסגרת חקיקה ראשית, ממנה יגזרו העקרונות להתקנות תקנות לעניין הכרטוס החכם, והתקנות יקבעו את דרך הפעולה של מערכת הכרטוס החכם ואת הנחיות רשם מאגרי המידע בהמשך. לדעתנו נדרשת עבודה רבה כדי למנוע פגיעה מיותרת בפרטיות הנוסעים. כמובן, נשמח להיות לעזר בכל הנדרש.

אנו ממליצים לקבוע את עיקרון ה-Privacy by design כעיקרון מנחה במסגרת החקיקה הראשית. זאת מעבר להמלצותינו הפרטניות הנוגעות לאפיון מחודש של המערכת, נושא הנמצא בימים אלו בדיונים בין משרד התחבורה ובין רשות למשפט, טכנולוגיה ומידע במשרד המשפטים.

בברכה,

יהונתן קלינגר, צבי דביר

התנועה לזכויות דיגיטליות

info@privacy.site.co.il

התנועה לזכויות דיגיטליות עוסקת בהגנה ובקידום זכויות פרט וקהילה בעידן הדיגיטלי. התנועה עוסקת בהגנה על הזכות לפרטיות, חופש הביטוי, הזכות לשוויון, זכויות צרכניות וכדומה, ומתייחסת לפגיעות אפשריות בזכויות אלה על-ידי טכנולוגיות המידע. בתנועה חברים מומחים מתחומים שונים, בעלי הבנה והכרה בכוחה הכפול של הטכנולוגיה לקדם מצד אחד זכויות פרט וקהילה ולפגוע בהן מצד שני. התנועה שמה לעצמה כמטרה להוות מוקד-ידע בנקודות ההשקה בין הטכנולוגיה וזכויות הפרט והקהילה, ולקדמן במסגרת פעולתה.