משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

מדריך הגנת הפרטיות לעיר החכמה

ינואר 2020

מהדורה מחודשת ומעודכנת

עקרונות להטמעת טכנולוגיות חדשות

תחבורה במרחב העירוני

תיק נתוני תושב

Not everything that is legally compliant and technically feasible is morally sustainable

Giovanni Buttarelli 1957-2019

לא כל מה שעומד בהוראות החוק ובעל ישימות טכנולוגית, הוא בהכרח גם מוסרי

ג'ובאני בוטארלי 1957-2019

ג'ובאני בוטארלי היה המפקח האירופאי הראשי על הגנת המידע בשנים 2014-2019, אשר הוביל את השינוי הדרמטי בחוק הגנת המידע הכללי האירופאי (GDPR) שנכנס לתוקף במאי 2018. שינוי גלובלי זה האיר באור גדול את הגישה החדשה לפרטיות ולהשלכות שלה בעידן המידע. ג'ובאני האמין כי יש להניע את היישום של הטכנולוגיות החדשות לכיוון הוגן ואתי יותר עבור אנשים ברחבי העולם, תוך שהוא טוען כי אפליה מקוונת אינה מסוג הדמוקרטיה שמגיעה לנו. ג'ובאני היה אדם אדיב ומסור לשליחותו ושימש כמנטור לרשויות הגנת הפרטיות בעולם כולו.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

מדריך הגנת הפרטיות לעיר החכמה

ינואר 2020

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

מדריך הגנת
הפרטיות
לעיר החכמה

תוכן עניינים

הקדמה 4
פרק 1 | העיר החכמה 6
תפישת העיר החכמה 6
מגמות בעולם ובישראל 7
עולמות התוכן של העיר החכמה 8
פרק 2 | פרטיות 10
הזכות לפרטיות על קצה המזלג 10
הרשות להגנת הפרטיות 11
פרק 3 | אתגרי פרטיות בערים חכמות 12
פרק 4 | החובות הכלליות בחוק ביחס לאיסוף ולשימוש במידע אישי 14
ניהול מאגרי מידע 14
תקנות הגנת הפרטיות (אבטחת מידע) 16
פרק 5 | עקרונות להטמעת טכנולוגיות חדשות במסגרת העיר החכמה 20
פרק 6 | הגנת הפרטיות בעיר החכמה - נושאים במיקוד 23
מצלמות מעקב ואבטחה 23
תחבורה במרחב העירוני 27
תיק נתוני תושב 31

מדריך זה מוגש כמידע כללי לשירות הציבור/בעלי תפקידים ברשויות המקומיות. הנוסח המחייב הוא הוראות חוק הגנת הפרטיות, התקנות שהותקנו מכוחו והנחיות הרשות להגנת הפרטיות.

הדוגמאות במדריך זה הובאו כדוגמאות כלליות בלבד המציגות אפשרויות ליישום התוכן המובא במדריך. הדוגמאות אינן מתאימות כפי שהן לכל מקרה, ויש לבחון כל מקרה וליישם את הוראות החוק בהתאם לנסיבותיו.

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

הקדמה

מדינת ישראל קבעה יעד לפיו כל רשות מקומית בישראל תהיה חכמה ובעלת תשתיות לפלטפורמות דיגיטליות[1], בין אם היא עיר או מועצה מקומית או מועצה אזורית. זאת מתוך ראייה אסטרטגית ארוכת טווח וההבנה כי, על פי הערכות, בעוד כעשור, 75% מאוכלוסיית העולם יתגוררו בערים וכי עד שנת 2030 יהיו בעולם 41 "גלובל מגה סיטיז" – ערים שמכילות 10 מיליון תושבים או יותר. על פי הערכת האו"ם, עד שנת 2050, כשבעה מכל תשעה אנשים בעולם יחיו בערים. כדי להתכונן לאתגר גדול זה, ערים בישראל ובכל רחבי העולם, פונות לטכנולוגיות מבוססות רשת ולניתוח מאגרי נתונים בכדי להפוך את עצמן לערים חכמות.

אין הגדרה אחת מוסכמת ל"עיר חכמה" (רשות מקומית בעידן הדיגיטלי) וכל עיר יוצקת תוכן להגדרה, בין היתר, בהתאם לערכים מרכזיים המתבססים על אלמנטים של **שיתוף התושבים** ושמיעת דעותיהם **והנגשת כלים דיגיטליים** עבורם, בכדי שאלה יוכלו לממש את זכויותיהם. לעיר החכמה מוגדרות מטרות נוספות כמו חיסכון בהוצאות, ניצול משאבים מיטבי ואספקת שירותים טובים יותר לתושבים. ההתפתחויות הטכנולוגיות, הסביבתיות והסוציולוגיות הובילו לשיפור באיכות החיים של התושבים בעיר החכמה אך יחד עם זאת הביאו גם להיווצרות איומים פוטנציאליים על זכותם לפרטיותם. למשל, היעדר הסכמה של התושבים לעיבוד נתונים אישיים, או סוגיות אחרות הכוללות את האופן שבו ערים חכמות אוספות נתונים פרטיים מאינטראקציות ציבוריות בלתי נמנעות, הפרטת הבעלות בתשתיות ונתונים, עיבוד מחדש של נתוני עתק (Big Data) שנאספו מהאזרחים, אחסון נתונים אלה בענן ועוד.

בערים חכמות יש פוטנציאל **לאוטופיה** עירונית, אך באותו זמן הן נושאות עמן זרעים של עולם **דיסטופי**. עולם בו קיימים מצלמות וחיישנים ברחבי העיר, עולם שבו מתקיימים ניטור מתמיד וכריית מידע אישי של תושבי העיר, עולם שבו מערכות מנתחות את ההתנהגויות והנטיות של התושבים.

בהינתן יתרונות וסיכונים משמעותיים אלו, האימוץ המהיר של טכנולוגיות עיר חכמה בישראל מעלה את השאלה: **כיצד יכולה העיר החכמה לאזן בין יתרונות של חברה עשירה במידע לבין צמצום האיומים על הזכות לפרטיות?**

מדריך זה מרכז מידע בנושאי הגנת הפרטיות, מכיל שיטות עבודה מומלצות ודוגמאות על מנת לסייע לרשויות המקומיות ולעובדיהן לנווט בנושאים מורכבים אלה, להבהיר את הדרך למציאת איזון נכון בין איסוף ועיבוד מידע לשמירה על הפרטיות ולפעול למען הגנה ושמירה על פרטיות התושבים בעיר הדיגיטלית המתפתחת.

1 | החלטת ממשלה 2733 מיום 11.6.2017

מהדורה מחודשת זו כוללת מבנה עדכני של המדריך הבנוי לצרכי הרשויות המקומיות ובאה להנגיש את חוק הגנת הפרטיות ותקנותיו ונספחיו כפי שרואה זאת הרשות להגנת הפרטיות. בשל כך, הוספנו במהדורה זו את עיקרי החובות הכלליות בחוק ביחס לאיסוף ושימוש במידע אישי ולאחר מכן את העקרונות להטמעת טכנולוגיות חדשות בעיר החכמה. עוד מחדש מדריך זה דפי מידע בדבר תחבורה במרחב העירוני ותיק נתוני תושב.

בחלקו הראשון כולל המדריך סקירה כללית באשר ל'מה היא עיר חכמה', מהי 'פרטיות' ומהם אתגרי הפרטיות בעיר החכמה.

חלקו השני מפרט ומסביר את הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות" או "החוק") בדגש על איסוף ושימוש במידע אישי.

בחלקו השלישי מפורטים עקרונות הגנת הפרטיות בעת הטמעת טכנולוגיות חדשות בעיר החכמה.

חלקו האחרון של המדריך כולל מידע בנושאים ממוקדים בצרכי רשויות מקומיות ובמיוחד בהתייחס להטמעת מערכות דיגיטליות.

מדריך זה אשר נכתב על ידי הרשות להגנת הפרטיות נועד לסייע לכם בניהול סיכוני הפרטיות עוד בשלבי תכנון של הטמעת שירותים דיגיטליים או טכנולוגיות חדשות בעיר החכמה. מטרתו להציג בתמציתיות את הדרישות הרלוונטיות בחוק הגנת הפרטיות ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות הגנת הפרטיות (אבטחת מידע)" או "התקנות") וכן הנחיות חשובות תוך סקירת מקרי בוחן מן העולם.

פרק 1 | העיר החכמה

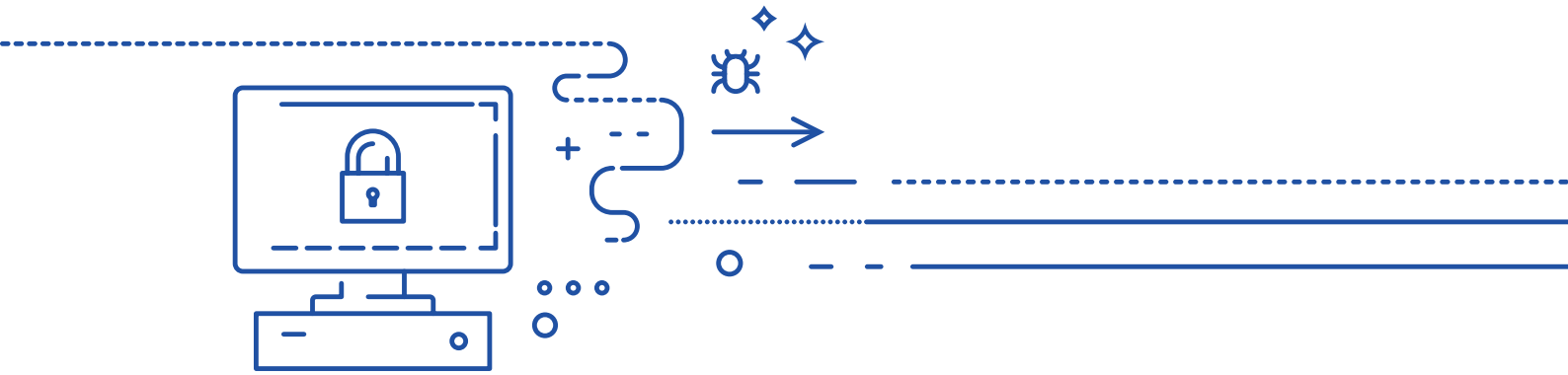
תפישת העיר החכמה

בשנים האחרונות אנו עדים להתחזקות מעמדן של ערים בתוך המערכת הלאומית והעולמית, כאשר נוצרות יותר ויותר ערי ענק (Mega Cities) חזקות ומבוססות, שבהן מתרכז העושר העולמי. פיתוח תפישת העיר החכמה ויישומה בעולם, מקודם על ידי ערי ענק אלו, אשר מובילות אסטרטגיה ומעודדות טרנדים ופיתוחים טכנולוגיים המהווים בסיס למידה עבור ערים, ממשלות ואף מדינות אחרות.

מכיוון שערים אלו גדולות וחזקות, הן מסוגלות למנף את נכסיהן הטכנולוגיים, לפתח את תפישת העיר החכמה וליישמה, לרוב בשיתוף הקהילה העסקית **ולטובת תושבי העיר ושיפור איכות חייהם**. כיום, לא קיימת כמעט עיר גדולה ומובילה בעולם שאינה משתמשת בטכנולוגיה כלשהי לניהול המתרחש בעיר, הביטחון בעיר, הקשר עם התושבים והענקת השירותים העירוניים.

למונח 'עיר חכמה' טווח הגדרות יחסית רחב, כאשר מדינות, ארגונים ורשויות שונות מגדירים אותו באופן שונה. עם זאת, **עיקר התפישה מתמקדת בשימוש בטכנולוגיות מידע ותקשורת, ככלי להשגת מטרות חברתיות וכלכליות בעיר**. כלומר, מדובר בתפישת ניהול עיר השואפת להשיג שימוש יעיל במשאבי העיר לצד שליטה ובקרה על הפעילויות בה, כל זאת לטובת:

1. רווחת התושבים, איכות חייהם וביטחונם.
2. הגדלת יעילות ואפקטיביות של גופי העיריה והרשויות הפועלים בעיר.
3. הגברת שגשוג וצמיחה כלכלית.
4. איכות סביבה וקיימות.



מגמות בעולם ובישראל

מקובל למנות שלושה שלבים באבולוציית הערים החכמות בעולם, אשר בעיקרה מתארת התפתחות ומעבר מהתמקדות בטכנולוגיה להתמקדות בתושבי הערים. הטכנולוגיה, שבעבר נתפשה כליבת העיסוק בעיר החכמה, נתפשת כיום כמאפשרת, כמסייעת וכתשתית לטובת שיפור איכות חיי התושבים בעיר:

1. **עיר חכמה 1.0 (Technology Driven)** - ערים המבקשות למקסם את השימוש בטכנולוגיה לטובת מינוף כלכלי והגברת יעילות ושליטה במתרחש בעיר. לרוב בערים מסוג זה, מי שהובילו את התפתחות ואימוץ הפתרונות היו ספקיות ענק מעולם הטכנולוגיה והטלקום ולא הרשויות המוניציפליות עצמן.
2. **עיר חכמה 2.0 (Technology Enabled, City-Led)** - בשלב זה, הרשות המקומית היא זו שמובילה אימוץ ואף יצירה של פתרונות טכנולוגיים בעיר החכמה, אך כאמצעי לשיפור איכות חיי התושבים.
3. **עיר חכמה 3.0 (Citizen Co-Creation)** - שלב זה בהתפתחות הערים החכמות הולך ותופס תאוצה כיום כאשר ערים חכמות מובילות בעולם מאמצות מודלים ליצירה משותפת עם תושביהן (וינה, ברצלונה, מדיין ועוד). מדובר ביוזמות של יצירת והטמעת פתרונות טכנולוגיים לטובת התושבים, אשר מתחילות "מלמטה" ל"מעלה", תוך מתן דגש על המימד הקהילתי, על שוויון והכלה חברתית וכלכלה מקומית ומקיימת.

בשנים האחרונות אנו עדים ליותר ויותר מיזמים בתחום ערים חכמות הנכנסים גם לערים בישראל. ההתעניינות בתחום חוצה ערים ורשויות, ואין כמעט עיר שאינה מגששת את דרכה בתחום מתפתח זה. השיח הציבורי סביב נושא הערים החכמות הולך ומתגבר, מספר הפרסומים והכנסים המקצועיים בנושא גדל מידי שנה ומיזמים של רשויות ועיריות גדולות המבקשות לאמץ שיטות וטכנולוגיות חדשניות מתפרסמים חדשות לבקרים. בנוסף לחלחול של טכנולוגיות חדשות וקיימות לערים בישראל, במקרים מסוימים טכנולוגיות אף מפותחות בגיבוי וביוזמה של הערים, במסגרת חזון מגובש ותכניות אסטרטגיות.

בהמשך למגמת צמיחה זו ולצורך ייעול תהליכי עבודה ושיפור השירות לתושבים בערי ישראל, החליטה הממשלה על קידום תפישת 'עיר חכמה', והטילה את הובלת התחום **בהיבט הדיגיטלי** על המשרד לשוויון חברתי וישראל דיגיטלית ועל משרד הפנים[2].

2 | ראה הערת שוליים 1 לעיל.

עולמות התוכן של העיר החכמה

בערים חכמות בעולם ניתן למצוא מאות מיזמים מסוגים שונים, הכוללים שימוש באמצעים טכנולוגיים בנושאים מגוונים – החל מפריסת מצלמות וחיישנים מסוגים שונים בעיר למטרות ניטור שונות כמו תחבורה, ביטחון, חיסכון באנרגיה וקיימות, דרך אפליקציות ופלטפורמות המוקמות מטעם העיריה במטרה לעודד תיירות או צמיחת תעסוקה מקומית ועד פלטפורמות שנועדו לעודד שיתוף של מידע עירוני, כלי רכב, ציוד וכדומה.

מתוך סקירה רחבה שבוצעה עבור הרשות ומיפוי המיזמים והנושאים הרבים בהם עוסקות ערים חכמות בעולם ובישראל, **סווגו והוגדרו שישה עולמות תוכן מובהקים שבהם מתמקדות הערים - חינוך, תחבורה, סביבה וקיימות, ביטחון ואבטחה, שירותים עירוניים וכלכלה.** תחת כל אחד מעולמות התוכן הללו, אוגדו והוגדרו קטגוריות של תחומים על בסיס מידת השכיחות שלהם בערים מובילות העולם.

לדוגמא, עולם התוכן הקשור בנושא התחבורה מאגד חמישה תחומים בולטים – תחום הנסיעות המשותפות, תחום התחבורה הציבורית, תחום ניטור ובקרת תנועה, תחום החנייה ותחום האכיפה והתשלום. עולם התוכן הקשור בשירותים עירוניים רחב גם הוא ומאגד חמישה תחומים – 'E-Muni', קהילה, רווחה ובריאות, תחזוקה ותפעול וממשל פתוח ומשתף. עבור כל אחד מעולמות התוכן נערכה סקירה של תתי-תחומים ומיזמים בולטים בערים חכמות.

תוצאות התהליך סייעו במיקוד בתחומים אליהם קיימת עדיפות להתייחס בטווח המידי:

עולמות התוכן של העיר החכמה

תחבורה
- אמצעי תחבורה והתניידות
- ניהול ובקרת תנועה
- חניה

ביטחון ואבטחה
- ביטחון שוטף
- אבטחת נכסים
- חירום ואירועים חריגים

חינוך
- סביבת למידה
- אוריינות ומיומנות דיגיטלית
- הנגשת מידע וידע

סביבה וקיימות
- איכות הסביבה
- אנרגיה ומים
- תברואה וניקיון

כלכלה
- מסחר ותעסוקה
- תיירות, תרבות ופנאי
- כלכלה שיתופית

שירותים עירוניים
- E-Muni
- קהילה
- רווחה ובריאות
- תחזוקה ותפעול
- ממשל פתוח ומשתף

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, מדגים החוק מהי פגיעה בפרטיות על ידי ציון מספר מצבים של פגיעה בפרטיות, כמו כניסה לרשות היחיד של אדם שלא בהסכמתו. יחד עם זאת, חוק היסוד קובע כי הזכות לפרטיות אינה זכות מוחלטת, והפגיעה בה כפופה לעמידה בתנאים מסוימים.

נוסף על מעמדה של הזכות לפרטיות כזכות יסוד חוקתית, נהנתה הזכות עוד לפני חקיקת חוק היסוד, להגנה מפורשת ונרחבת בחוק הגנת הפרטיות. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות תהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית שעונשה חמש שנות מאסר. אחד מעקרונות הבסיס של החוק הוא דרישת ההסכמה. החוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק לא מגדיר מהי הסכמה אלא רק מציין כי 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 5 למדריך זה העוסק בנושא.

מכוח החוק הותקנו תקנות וצווים בעניינים שונים, ובהם תקנות הגנת הפרטיות (אבטחת מידע).

הרשות להגנת הפרטיות

הרשות להגנת הפרטיות הינה רשם מאגרי המידע הגוף המהווה את הגוף המסדיר, המפקח והאוכף על פי הוראות פרק ב' לחוק הגנת הפרטיות התשמ"א – 1981 על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי.

במסגרת תפקידה של הרשות כרגולטור של הזכות להגנת הפרטיות ולהגנת מידע אישי בישראל, הרשות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים מכוח חוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. הרשות פועלת להשגת מטרה זו באמצעות התווית 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 וחיזוק תחושת המוגנות של הציבור. כל זאת, במטרה לצמצם את הסיכונים הגוברים לפגיעה בפרטיות בעת שמירת מידע דיגיטלי, בעיבודו ובניהולו, והכל תוך איזון ומתן משקל ראוי לחידושים הטכנולוגים וליתרונותיהם עבור השוק והמשתמשים.

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

פרק 3 | אתגרי פרטיות בערים חכמות

ערים רבות בעולם משקיעות כאמור משאבים אדירים לצורך הפיכתן לערים חכמות ודיגיטליות. על אף יתרונות רבים שגלומים בעיר החכמה עבור מגוון השותפים (תושבים, הרשות, עסקים ועוד), ישנם אתגרים וסיכונים לא מעטים לפרטיותם של התושבים המתגוררים בערים החכמות, אליהם הרשויות והעיריות להיות מודעות.

שיתוף מידע אישי, אשר בעבר נעשה בצורה 'אופקית' בין אנשים הופך יותר ויותר 'אנכי', כאשר תושבים נאלצים לשתף מידע רב עם גופים כמו הרשות המקומית. למשל, אם בעבר התבקש התושב על ידי הרשות המקומית למסור מידע על הרגלי הצריכה שלו או הרגלי החנייה שלו וזאת לצרכי שיפור השירות, בעיר החכמה הרבה פעמים מידע שכזה לא נמסר על-ידי התושב אלא נאסף עליו באופן עקיף וחד-צדדי באמצעים טכנולוגיים, ומעובד, מנותח ומתועל למאגרים קבועים שבבעלות העיריה. כלומר, אם בעבר זליגת מידע אישי ופגיעה בפרטיות היתה יכולה ל"הסתכם" ברכילות, מבוכה או סנקציות חברתיות על הפרט, העיר החכמה משקפת את אתגרי "הדור הבא" של הפרטיות ו"מחירים" חמורים יותר. אנו חיים בעידן שבו הטכנולוגיות מאפשרות **מעקב תמידי אחר התושב, שלל שימושים במידע שנאסף, והפקת תובנות נוספות מהמידע**. תוצאות המציאות הזו עשויות להיות לטובת התושבים והחברה, אך יתכנו גם היבטים שליליים שיש להביא בחשבון כעודף התערבות מצד העירייה בחיי התושבים, הגברת המישטור שיוביל לצעדי אכיפה וענישה ופגיעה במרקם החיים האינדיבידואלי המשגשג דווקא בהיותו בלתי מפוקח ובלתי מנוטר.

איסוף מידע באמצעות מצלמות וחיישנים מסוגים שונים משמש ערים חכמות כבר כיום לייעול תהליכי עבודה פנימיים, שיפור השירותים לתושבים וכן שמירה על בטיחותם וביטחונם.

היתרונות הרבים הגלומים באיסוף מידע שכזה אינם במחלוקת, עם זאת הם גם מהווים **בסיס למנגנוני מעקב ציבורי תמידי, אשר עלולים לפגוע בפרטיות התושבים**.

בעיר ניו יורק, לדוגמא, נתגלה כי סנסורים חכמים הפזורים בעיר קוראים את כרטיס ה- 'EZ-Pass' של התושבים ללא ידיעתם וכך אוספים מידע לגביי מיקומם של כלי רכב. במקור כרטיס זה אמור לשמש לשם מעבר מהיר במחסומים של כבישי אגרה, כפי שסביר שמרבית המשתמשים בו הניחו, אולם בו בזמן התברר כי נאסף מידע אודות מיקום המשתמשים, דבר העלול לפגוע בפרטיותם.

הקו הדק שבין ניטור התנהגות לבין הרצון להכתיב אותה הולך ומיטשטש. ערים חכמות עוסקות כבר כיום בהכוונת התנהגות תושבים, בין אם מדובר בשינוי הרגלי צריכת אנרגיה ומים לטובת הגברת הקיימות, שינוי הרגלי חניה, נהיגה ונסיעה לטובת הפחתת עומסי תנועה בעיר או שינוי

הדרך שבה תושבי העיר הצעירים לומדים ומתחנכים. יתכן שדוגמאות אלו יביאו להטבה באיכות חייהם ורווחתם של התושבים, אך ללא חשיבה, בקרה והצבת גבולות, יתכנו גם שימושים במידע שייאסף על אנשים אשר לא יהיו לטובתם ויפגעו באינטרסים שלהם.

אתגר נוסף שעומד בפני הרשויות המקומיות בהיבט הפרטיות, הוא **היעדר אלטרנטיבה**. בשוק הפרטי מודל עסקי של חברות רבות מאפשר מתן שירות או מוצר בתמורה למידע שנמסר על ידי המשתמש, וזאת מכיוון שמידע אישי רב על משתמשים מהווה לרוב יתרון תחרותי. בהנחה שהדבר הובא לידיעתם, למשתמשים אלה יש מידה מסוימת של שליטה מתי, איך ועד כמה הם מוותרים על המידע האישי שלהם בתמורה לשירותים.

לעומת זאת, ל'משתמשי' העיר החכמה (התושבים) **אין אלטרנטיבה לקבלת שירותים ציבוריים והם אינם יכולים להימנע מאיסוף המידע עליהם מבלי ש"ישלמו" על כך, בין היתר, בביטחון ובאיכות החיים**, בפרט כאשר מדובר במידע שנאסף בתשתיות עירוניות חיוניות, כמו במערכת רכבות יחידה בעיר, מערכת החשמל ומערכות המים וכו'. בכך עשוי להתערער יסוד ההסכמה של התושב לשימושי הרשות במידע על אודותיו, מאחר שאין לו אפשרות לבחור בחלופה אחרת. על כן, מתחייבת זהירות רבה יותר של הרשות בדרישה לשימוש במידע אישי של תושביה.

בנוסף למחסור בכוחות שוק תחרותיים שעשויים לסייע בשמירה על הפרטיות בעיר החכמה, איסוף המידע שמבצעת הרשות המקומית **מאתגר גם את עקרון צמידות המטרה.** לא תמיד ברור האם השימוש שנעשה במידע הנאסף על-ידי העיריה הוא אכן למטרה שהוגדרה ולה בלבד. ישנן דוגמאות מערים בעולם שבהן מידע שהצטבר בידי השלטון המקומי "נדד" גם לרשויות אחרות (שלטון מרכזי או רשויות אכיפת החוק) ואף לגורמים מסחריים, ושימש למטרות שאינן המטרות אשר לשמן אישר התושב את איסוף המידע עליו או שהעירייה רשאית הייתה לאסוף ולהשתמש בו מתוקף סמכותה על פי דין.

לדוגמא, תושב המשתמש בפלטפורמה עירונית המאפשרת לדווח על מפגעים תשתיתיים בעיר באמצעות העלאת תמונות, יתכן שהיה בוחר שלא להעלותן לו היה מודע לשימוש שנעשה במידע, ככל שנעשה, מעבר לשימוש הספציפי במידע שהעביר למטרה שלשמה הועבר.

אתגר נוסף לרשויות המקומיות בעת הטמעת עיר חכמה, הוא **ריבוי המידע המצטבר במאגריה המגדיל את הצורך של הרשות המקומית להשקיע באבטחת מידע, על מנת למנוע דליפת מידע אישי של התושבים.** בנוסף, מאגרי המידע הללו עשויים **להוביל לניתוחים מוטים והסקת מסקנות לא נכונות** ואף עלולים להביא להקצאת משאבים לא נכונה, לאפליית אוכלוסיות מסוימות ואף לצעדים לא אתיים הפוגעים בחרויות הפרט ובשוויון.

טכנולוגיות הניטור השונות והניבוי האנליטי מייצרות אתגרים לפרטיות, אך הן עשויות גם להיות חלק ממסגרת המייצרת ערך רב לתושב ולעירייה, יחסי אמון עם הרשות המקומית והעצמת אוכלוסיות. על אף אתגרי הפרטיות הרבים והמורכבים העומדים בפני הרשות המקומית והתושבים בערים חכמות, **ישנן דרכים רבות למזעור אתגרים אלה ולניהול הסיכונים** באופן מושכל המאפשר הגנה על פרטיותם של התושבים.

פרק 4 | החובות הכלליות בחוק ביחס לאיסוף ולשימוש במידע אישי

פרק זה מפרט את הדרישות הבסיסיות שמטיל החוק על איסוף ושימוש במידע אישי. דרישות אלה רלבנטיות גם ביחס לטכנולוגיות המשמשות את הערים החכמות וגם ביחס למאגרי המידע הנוצרים במסגרת השימוש בהן.

ניהול מאגרי מידע

בערים החכמות, **מצטברת כמות עצומה של מידע במאגרים שונים**. החל ממאגרים בסיסיים המכילים מידע על תושבי היישוב, כמו מאגר הארנונה העירוני או מאגרי נתוני החינוך העירוניים ועד מאגרים הייחודיים לערים החכמות, כמו מאגרי מידע המצטברים מרשת ה-WiFi העירונית, מכרטיסי התושב המקומיים או מאפליקציות שונות שמפעילה הרשות המקומית או העיריה לטובת התושבים, לעיתים קרובות באמצעות גורמים חיצוניים וקבלני משנה.

מאגרי מידע אלה, המגיעים ממקורות רבים, מצטלבים בנקודה מסוימת ומחייבים את הרשות או העיריה לנהלם בצורה מאובטחת, תוך הקפדה על דגשי ניהול מאגרי מידע ותקנות אבטחת מידע, על מנת למנוע זליגת מידע אישי של תושבים.

למעט מספר חריגים מצומצם, מאגר מידע הוא 'אוסף נתוני מידע על אדם הניתן לזיהוי והמוחזק באמצעים דיגיטליים', כמוגדר בחוק הגנת הפרטיות, תשמ"א-1981.

במסגרת פרק ב' לחוק, נקבעו הוראת לעניין הגנה על הפרטיות במאגרי מידע, בין היתר בהיבטי חובת הרישום של המאגרים באמצעות רשם מאגרי המידע (הרשות להגנת הפרטיות), אופן החזקת המאגרים, זכויות האנשים שעליהם נאסף ונשמר המידע (המכונים 'נושאי המידע') וכן השימושים המותרים במידע השמור במאגרים השונים.

1. **חובת הרישום** – בנסיבות מסוימות, המפורטות בסעיף 8(ג) לחוק, נדרש בעל מאגר מידע לרשום את המאגר אצל הרשות להגנת הפרטיות. מאגר מידע של רשות מקומית בישראל חייב ברישום, שכן מדובר בגוף ציבורי על פי הוראות החוק.
2. **אין לעשות שימוש במידע שלא למטרה שלשמה נמסר ונאסף** – מחובתה של הרשות המקומית לעמוד בעקרון 'צמידות המטרה', אשר קובע כי **ניתן לעשות שימוש במידע הנאגר אך ורק לטובת המטרה שלשמה הוא נאסף ולא לשם אף מטרה אחרת** (סעיף 8(ב)).

דוגמה

עיריית סן פרנסיסקו מקדמת מיזמי תעסוקה לאוכלוסיות מוחלשות בעיר, ועל כן יצרה פלטפורמה עירונית מקוונת אשר מתאימה בין בתי עסק וחברות המחפשות עובדים בעיר, לבין תושבים המחפשים תעסוקה בתחומים שונים.

אפליקציות מסוג זה, לרוב **מכילות מידע אישי רגיש** על מועסקים פוטנציאליים (קו"ח מפורטים, שנות ותק, השכלה ועוד), ולכן **העיריה נוקטת משנה זהירות** בכל הנוגע למידע זה, ומשתמשת בו **תוך יידוע וקבלת הסכמתם של התושבים לשימוש במידע לטובת המטרה שלשמה נאסף בלבד,** ולא לטובת הצעות ערך אחרות שיתכן וניתן היה להציע לאוכלוסייה מסוג זה ב"דחיפה" (למשל, השתתפות במיזמי דיור ציבורי שמקדמת העיריה וכדומה).

3. **חובתו של בעל מאגר המידע לעמוד על זכויותיהם של 'נושאי המידע'** (האנשים עליהם נאסף ונשמר המידע):

- **חובת מתן הודעה** – העיריה מחויבת ליידע את הפרט, בטרם איסוף המידע, האם מחובתו החוקית למסור את המידע או לא (למשל, לצורך קביעת גובה מיסי ארנונה, התושב מחויב למסור מידע רלוונטי), מה המטרה שלשמה נאסף המידע, למי יימסר המידע ומה תהיה מטרת המסירה (לפי סעיף 11 לחוק).
- **זכות עיון במידע** – חובת העיריה לאפשר לכל פרט עליו נאגר מידע, את זכות העיון בנתונים שנאספו עליו, תחת כמה מגבלות (המפורטות בסעיף 13 לחוק).
- **זכות תיקון המידע** – נושא המידע רשאי לדרוש תיקון של מידע אודותיו, ככל שהמידע במאגר אינו נכון (כמפורט בסעיף 14 לחוק).
- **חובת הסודיות** – בעל מאגר המידע, המחזיק בו ומי מעובדיו, מחויבים בשמירת סודיות המידע אליו נחשפו כחלק מעבודתם (סעיף 16 לחוק).

4. בנוסף, **בעת פנייה לתושבים בדיוור ישיר**, מחויבת העיריה להקפיד על עמידה במספר כללים הנגזרים מחוק הגנת הפרטיות ומובאים בהרחבה בהנחיה בנושא דיוור ישיר ושירותי דיוור ישיר[3].

5. **חובה נוספת של בעל מאגר המידע והמחזיק בו, היא חובת אבטחת המידע** (המפורטת בסעיף 17 לחוק) וכן עמידה בתקנות הגנת הפרטיות (אבטחת מידע).

3 | ראו הנחיית רשם מאגרי המידע מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר" באתר הרשות להגנת הפרטיות

תקנות הגנת הפרטיות (אבטחת מידע)

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

בפרק זה מובאים בתמצות העקרונות המרכזיים של אבטחת המידע במאגרי המידע של הרשות המקומית, בהתאם לחובות המפורטות בתקנות. הרשות המקומית מחויבת להקפיד על יישום עקרונות אלה באופן שוטף, וכן בטרם הטמעת טכנולוגיות ומיזמים שונים של עיר חכמה.

מחובת כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה. בהתאם להגדרת רמת האבטחה של המאגר תבחן הרשות המקומית אילו תקנות חלות על המאגר. **מאגר שבבעלות גוף ציבורי, כמו רשות מקומית, חלה עליו רמת האבטחה הבינונית, לכל הפחות. רמת האבטחה הגבוהה תחול על מאגר שבבעלות גוף ציבורי כאשר הוא מכיל מידע אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה לעיון ופעולות בו עולה על 100 מורשים אשר מטרתו העיקרית היא לדיווח ישיר, או 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.**

דוגמה

בעיר תל-אביב יפו, מאגר נתוני התלמידים במערכת החינוך מכיל מידע אודות פרטיהם האישיים (אשר יכולים, בין היתר, לכלול מידע רפואי, וסוציואקונומי) של כ-80 אלף תלמידים. על כן, במידה ומספר מורשי הגישה למאגר אינו עולה על 100 **מאגר זה יוגדר ברמת אבטחה בינונית**.

לעומת זאת, בהנחה ומספר מורשי הגישה למאגר נתוני התלמידים של עיריית תל אביב עולה על 100, **מאגר זה יוגדר ברמת אבטחה גבוהה**, וזאת לאור היקף מורשי הגישה וסוג המידע אשר מופיע בו.

נתונים: שנתון סטטיסטי עיריית ת"א יפו, 2016 – לוחות 6.1 ו-15.1

בהמשך, לאחר שנבדקה והוגדרה רמת האבטחה הנדרשת למאגר המידע, יש לפנות לטבלת הסבר המפרטת אילו תקנות חלות על המאגר[4]. **להלן מובאות בתמצות התקנות הרלוונטיות למאגרים עליהם חלות רמות האבטחה הבינונית והגבוהה:**

1. **חובת הרשות המקומית לנהל 'מסמך הגדרות מאגר', לכל מאגר בכל רמת אבטחה**, וזאת בהתאם לתקנה 2 לתקנות הגנת הפרטיות (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 (לדוגמא: איסוף מידע על קיבולת אפשרית ומידת תפוסה של פחי אשפה פרטיים וציבוריים בעיר, באמצעות חיישני תהודה), תיאור **מטרות איסוף המידע** (למשל: לשם ניתוח המידע ויצירת אופטימיזציה בבחירת מסלולי איסוף ופינוי האשפה בעיר), **תיאור סוגי המידע** השונים הכלולים במאגר (למשל: שם בעל הפח, כתובתו, מיקום מדויק של הפח כעת, רמת תפוסה נוכחית, רמת דחיפות הפינוי באזור), פרטים על העברת מאגר המידע או **שימוש מחוץ לגבולות ישראל** (למשל: המידע אינו מועבר לחו"ל ומעובד במאגרים המצויים על שרתי הרשות המקומית), האם נעשה **עיבוד באמצעות גורם זר או חיצוני** (לדוגמא: על אף שהמאגר מוחזק בשרתי העירייה, המיזם ופלטפורמת עיבוד המידע מופעלות על ידי חברת "XYZ", המשמשת כספק חיצוני בהסכם עם העירייה), **מיפוי סיכונים** אפשריים ודרכי התמודדות עמם (למשל: סיכון לזליגת מידע דרך הגורם החיצוני, עימו ניתן יהיה להתמודד באמצעות ביקורות יזומות מטעם ממונה אבטחת המידע של העירייה), **פרטים אישיים** של מנהלת המאגר, מחזיק/ת המאגר וממונה אבטחת המידע.

2. **חובת הרשות המקומית למנות ממונה אבטחת מידע**, כמוגדר בתקנה 3 (וכן סעיף 17ב (א) לחוק). תנאים ודגשים ספציפיים מובאים בהרחבה במדריך תקנות הגנת הפרטיות.

3. **חובת הרשות המקומית 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 מוגדרת בתקנה 4[5].

4. **הרשות המקומית מחויבת לבצע מיפוי של מערכות המאגר וכן סקר סיכונים**. כלומר, 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 במדריך המלא. **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 | דגשים ספציפיים לכתיבת ולשמירת הנוהל מובאים בהרחבת באתר הרשות להגנת הפרטיות.

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

6. **הרשות המקומית מחויבת למזער את הסכנה הפוטנציאלית שמציב הגורם האנושי** באמצעות העסקת עובדים אשר עברו הכשרות מתאימות בתחומי אבטחת המידע. בנוסף, **מחובת הרשות המקומית לבחון את מידת התאמתם של העובדים הקיימים ולהעבירם סמינרים והדרכות אחת לשנתיים**, לכל הפחות. בתוך כך, על הרשות המקומית **לנהל הרשאות גישה למאגריה** בצורה מסודרת ואחראית, כמפורט בתקנות 7 ו-8 במדריך המלא.

7. **הרשות המקומית מחויבת לוודא שעובדים להם קיימת גישה למאגר הם אכן עובדים המורשים 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 לתקנות ובמדריך המלא.

8. **חובתה של הרשות המקומית לתעד אירועי אבטחה 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", **מחויבת הרשות המקומית להודיע לרשות להגנת הפרטיות באופן מיידי על כך**, וכן לדווח על הצעדים שננקטו בעקבות האירוע. ניתן לדווח באופן מקוון באתר האינטרנט של הרשות.

9. **הרשות המקומית מחויבת להקפיד על מניעת זליגת מידע בעת שימוש בהתקנים ניידים** (מחשבים ניידים, טלפונים חכמים וכד'), במידת הצורך האמצעות 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 הרשות המקומית לנקוט באמצעי אבטחה נוספים שימנעו גישה חיצונית ולא מורשית למידע** (תקנה 14).

10. **חובת הרשות המקומית 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 יש לבחון את סיכוני אבטחת המידע האפשריים, ובמידה והם גבוהים מידי יש להימנע ממיקור חוץ (ראו פירוט בפרק 6 למדריך זה). כמו כן, יש לקבוע בהסכם מפורש עם הספק החיצוני קווים מנחי לפעילותו, בין היתר: סוג המידע אותו רשאי לעבד, מערכות אליהן רשאי לגשת, חובתו לסודיות ועוד (כמפורט בתקנה 15 וכן בהנחיית הרשות להגנת הפרטיות בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי).

11. **הרשות המקומית מחויבת לערוך ביקורת פנימית או חיצונית, אחת ל-24 חודשים לפחות**, באמצעות גורם בעל הכשרה מתאימה, שאינו הממונה על אבטחת המאגר מטעמה, על מנת לוודא עמידה בתקנות, כמפורט בתקנה 16. במאגרים עליהם חלה רמת אבטחה גבוהה, ניתן לבצע ביקורת במסגרת עריכת סקר סיכונים (כמוסבר בתקנה 5).

12. **הרשות המקומית מחויבת 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 המאגר**. כמו כן, מוזכר כי לרשות להגנת הפרטיות שמורה הזכות לפטור מאגרים ספציפיים מחובות אבטחת מידע מתוך התקנות, או לחלופין להטיל חובות נוספות בהתאם לנסיבות, כמפורט בתקנות 19-20.

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

פרק 5 | עקרונות להטמעת טכנולוגיות חדשות במסגרת העיר החכמה

בפרק הקודם הוצגו העקרונות המחייבים הבסיסיים בחוק הגנת הפרטיות בנוגע לאיסוף ושימוש במידע אישי. עקרונות אלה מחייבים גם ביחס לטכנולוגיות המצויות בשימוש בערים החכמות ולמאגרי המידע הנוצרים תוך כדי שימוש בהן. **בפרק זה נפרט עקרונות נוספים אותם על הרשות המקומית ליישם כדי להתמודד עם הסיכונים המוגברים לפרטיות בעיר החכמה – סיכונים הנובעים מן המאפיינים הייחודיים של שימוש בטכנולוגיות מידע** במרחב העירוני, אשר תוארו והודגמו בפרקים הקודמים (פרקים 3 ו-4) למדריך.

על רשויות מקומיות לפעול בהתאם לעקרונות אלו בטרם מתקבלת החלטה על שימוש במיזם דיגיטלי חדש או רכישה של טכנולוגיה או מערכת מידע חדשה. המלצתנו היא לקרוא עקרונות אלו כמבוא לדפי המידע הספציפיים בנושאים ובטכנולוגיות שהרשות תפרסם ותעדכן מעת לעת.

אחד מיסודות הניהול הנכון של טכנולוגיות העיר החכמה טמון בהפנמה מוקדמת של שיקולי פרטיות באמצעות "אחריותיות" (Accountability) וגישה מתכללת. **הרשות המקומית נדרשת לנקוט באמצעים ארגוניים, טכנולוגיים ומשפטיים שישפרו את מידת ה"אחריותיות" והמחויבות שלה לצמצום ההשלכות של הטכנולוגיה על פרטיות התושבים**. מדובר באמצעים שהפכו לפרקטיקה מקובלת בערים החכמות בעולם, ובמקומות רבים כגון באיחוד האירופי, גם ללא דרישה חוקית ורגולטורית מפורשת. גם בישראל, ללא יישום עקרון האחריותיות, לא תצליח הרשות המקומית לכבד את הזכות החוקתית של תושביה לפרטיות, ותתקשה להימנע מפגיעה בפרטיותם במידה העולה על הנדרש.

ניהול מתכלל

1. ראשית, יש למנות ברשות המקומית גורם בכיר שיהיה אחראי לקביעת מדיניות כוללת בעניין השימוש במיזמי טכנולוגיות מידע ברשות 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 המופעלות בעיר ומהצלבת המידע הנאסף תוך כדי הפעלתן במקביל. לכן, נדרשת יד מכוונת ונקודת מבט מערכתית לשם הערכה מדוייקת של הסיכונים לפרטיות והטיפול בהם.

2. במידה וקיים ברשות המקומית 'ממונה הגנת פרטיות' (DPO), מומלץ שהוא יהיה אחראי על המשימה. 'ממונה הגנת פרטיות' הוא תפקיד שונה מתפקיד 'ממונה אבטחת המידע', שעל פי הוראות חוק הגנת הפרטיות קיימת חובה למנות בגופים ציבוריים לרבות ברשויות מקומיות. תפקיד 'ממונה הגנת הפרטיות' הוא בד"כ נושא משרה בכיר המרכז ועוסק בכל הצדדים המשפטיים של הגנת המידע האישי ברשות, ובמידת הצורך מנחה גם את ממונה האבטחה.

3. אם לא מונה ברשות המקומית עובד ייעודי הנושא בתפקיד ממונה הגנת פרטיות, ניתן להטיל את תכלול היבטי הפרטיות הקיימים בפרויקטים של העיר החכמה על ועדת היגוי ייעודית, צוות קבוע של ההנהלה הבכירה, וכדומה.

תסקיר – בחינה מוקדמת של ההשפעה על הפרטיות

4. הסיכונים הייחודיים והמוגברים לפרטיות התושבים ברשות מקומית אשר עושה שימוש בטכנולוגיות מידע באופן שיטתי - מקנים משנה חשיבות לצורך להקדים לקבלת ההחלטה על שימוש בטכנולוגיה עריכת "תסקיר השפעה על פרטיות" (Privacy Impact Assessment). "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, ומהווה אמצעי יעיל למימוש החובות שמטיל החוק על בעל מאגר. כמו כן, יצויין כי חלק מרכיבי התסקיר חופפים לדרישות הקיימות בסעיפים 2 ו–5 לתקנות הגנת הפרטיות (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 תיישם הרשות המקומית את תפיסת 'העיצוב לפרטיות' (Privacy By Design או PBD) וקונספט 'פרטיות כברירת מחדל' (Privacy by Default) (שיכונו להלן ביחד – עיצוב לפרטיות), הדוגלים 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.

שקיפות ושיתוף הציבור

7. על הרשות המקומית להקפיד לנהוג בשקיפות ולהביא לידיעת הציבור 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 לציבור התושבים האם יש באפשרותם לבחור להימנע מאיסוף המידע, כגון בדרך חלופית לקבלת שירות עירוני או שימוש בתשתית עירונית שלא כרוכה באיסוף של מידע אישי.

8. את המידע יש לפרסם במתכונת נגישה וברורה שתאפשר לתושבים לקבל החלטות מושכלות בדבר אופן השימוש בשירותי הרשות המקומית ומתקניה. רצוי שהמידע הרלבנטי יהיה נגיש הן בסמוך לשירות או לחיישן הנוגע בדבר, והן באופן מרוכז, למשל באיזור ייעודי באתר האינטרנט של הרשות המקומית או באפליקציה שלה.

9. השקיפות איננה רק עניין של מינהל תקין. היא נדרשת גם לפי הוראות חוק הגנת הפרטיות, וצפויה להגביר את אמון הציבור ברשות המקומית ובטכנולוגיות בהן היא משתמשת. קבלת עמדות הציבור ביחס לטכנולוגיות ולשימוש תסייע לרשות המקומית אף להעריך נכונה את הסיכונים והקשיים במסגרת עריכת תסקיר, ולעצב את המערכות באופן שימקסם את ההגנה על פרטיות התושבים.

שימוש במיקור חוץ ושיתוף פעולה עם גורמים מסחריים

10. במקרים רבים תושבי העיר או מבקריה מהווים מעין "קהל שבוי" החסר את האפשרות להימנע משימוש בשירות או בתשתית עירונית הכרוכים באיסוף מידע אישי. מסיבה זו, וכן בשל רגישות המידע שניתן להסיק מההיקף הגדול והמגוון של הנתונים הנאספים, נדרשת הרשות המקומית להקפדה יתרה בשיתופי פעולה עם גורמים מסחריים.

11. ראוי שההחלטה בנושא זה תתקבל בדרגים הבכירים ביותר של הרשות המקומית.

12. מכרזים או חוזים הנערכים בין הרשות המקומית לגורמים מסחריים בנוגע לפרויקטים הכרוכים בהפעלת טכנולוגיית מידע, חייבים לכלול התייחסות מפורטת להיבטי פרטיות ואבטחה, בין השאר בשים לב להנחיות רשות הגנת הפרטיות ולהוראות תקנות הגנת הפרטיות (אבטחת מידע) בנושא מיקור חוץ.

פרק 6 | הגנת הפרטיות בעיר החכמה - נושאים במיקוד

מצלמות מעקב ואבטחה

בעשורים האחרונים גובר השימוש באמצעים טכנולוגיים המיועדים לפיקוח ולמעקב חזותי וקולי מרחוק על שטחי ציבור. שימוש זה בא לידי ביטוי בהצבת מצלמות זעירות במקומות רבים במרחב הציבורי. טכנולוגיות אלה, הנקראות Surveillance Video או Closed Circuit Television (CCTV), הן בעלות השפעה מהותית על המרחב הציבורי והשימוש בהן כרוך בפגיעה בפרטיות. מצלמות מעקב משמשות ערים 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. במרחב ציבורי זה, תחושת המעקב התמידית הופכת מוחשית מאי פעם.

השפעה זו עשויה להיות חיובית, כאשר היא מצמצמת התנהגות עבריינית או בזבזנית המזיקה לזולת ולחברה כולה. מנגד, ההשפעה עלולה להיות שלילית, כאשר חלק ניכר מהפעילויות הנתפסות באמצעי התיעוד הדיגיטליים הן פעילויות שגרתיות ותמימות, שאינן מהסוג שהחברה מבקשת למנוע. בנוסף, ההתפתחויות ביכולת עיבוד הנתונים, דוגמת זיהוי פנים אוטומטי, זיהוי לוחיות רישוי, כמו גם ניתוח התוכן המצולם (למשל, ניתוח דפוס 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 התושבים.

אי לכך, פרסמה הרשות להגנת הפרטיות בשנת 2012 הנחיה בנושא 'שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן'. הנחייה זו מבהירה את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הפרטיות, שהפרתם עלולה להביא לצעדי אכיפה מנהלית ואף להגיע לכדי עבירה פלילית.

להלן מובאים בתמצות קווים מנחים ועקרונות מרכזיים בעת הטמעת טכנולוגיות של פיקוח ומעקב חזותי באמצעות מצלמות, וכן בניהול מאגרי המידע והצילומים הנקלטים בהן[6].

6 | הנוסח המלא והמחייב הוא הנוסח המופיע בחוק ובהנחיה בנושא 'שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן'.

1. **תכלית הצבת המצלמות ושמירה על עקרון צמידות המטרה והמידתיות** – בטרם הצבת מצלמות ברשות המקומית ושימוש במערכות ניתוח תמונה, כחלק ממיזמי עיר חכמה וככלל, **מחובת הרשות המקומית לוודא כי נערך תסקיר השפעה על פרטיות**. באחריות הרשות המקומית לוודא כי אכן נערכת בדיקה מקיפה הבוחנת את השלכות השימוש במצלמות על זכות הציבור לפרטיות, תוך התייחסות לנושאים הבאים:

- **תכלית הצבת המצלמות – מטרת הצבת המצלמות חייבת להיות מוגדרת באופן חד, ספציפי ומפורש**. לדוגמא – "מצלמות ניטור ומעקב תנועה, אשר אוספות מידע ומנתחות אותו בזמן אמת לשם ייעול מערך התנועה העירוני והגדרת מדיניות תחבורתית בעיר". **על המטרה להיות בעלת בסיס עובדתי** – כלומר, קשורה לבעיה שפתרונה דורש הצבת מצלמות. כמו כן, יש לוודא מראש כי המטרה אותה מבקשים להשיג היא אכן בתחום סמכותה של הרשות המקומית. **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 **הצבת מצלמה בידי רשות ציבורית מחייבת עמידה במבחן המידתיות**: 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 לתושב עולה על "העלות" במונחי הפרטיות? האם ניתן להשיג את המטרה באמצעים פחות פוגעניים? אמצעיים נוספים למזעור פגיעה בפרטיות ודגשים בנושא שמירת הצילומים ומחיקתם ניתן למצוא בהנחיית הרשות להגנת הפרטיות.
- **דגשים נוספים –**

- יש לנקוט משנה זהירות כשמדובר במצלמות המנטרות אוכלוסיות מוחלשות כמו קטינים או קשישים (קירבה למוסדות חינוך או סיעוד וכד').
- בנוסף, מומלץ לקבל החלטה על הטמעת טכנולוגיות מסוג זה בשיתוף הציבור ולקיים שימוע ציבורי שיאפשר לתושבים להביע את עמדותיהם, וכן לחברם למיזמים המקומיים של העיר החכמה.
- יש להיזהר במיוחד משימוש במצלמות מעקב לצורך הקלטה קולית. על מעקב קולי, הנתפס כרגיש וחודרני, חלות חובות מחמירות כמפורט בחוק האזנת סתר, התשל"ט-1979, שהפרה של הוראותיו מהווה עבירה פלילית חמורה.

2. **'תכנון לפרטיות'** – בעת הטמעת מיזמי עיר חכמה המשלבים מצלמות, **חובת הרשות המקומית להקפיד על 'תכנון לפרטיות' של המערכת, ולוודא כי מספר פרמטרים עומדים במבחן הרלוונטיות למטרה** ולתכליתן של הצבת המצלמות. למשל: **מיקום וזווית המצלמות** – כך שלא יאסף מידע יותר מהמינימום הנדרש. **מספר המצלמות** – לא יותר מהמינימום הנדרש. **זמני צילום** – למשל, במידה ומדובר במצלמות לניתוח תנועה וניתובה, להפעילן בשעות עומסי התנועה בלבד. **רזולוציה** – למשל, אם מטרתו המוגדרת של מיזם היא לנתב תנועת כלי רכב, הכולל צורך לזהות לוחיות רישוי, ומכאן שיש הצדקה בשימוש בצילום ברזולוציה גבוהה. מנגד, מיזם תאורה חכמה שנועד לחסוך בצריכת אנרגיה עירונית אינו מחייב צילום ברזולוציה גבוהה.

3. **בנוסף, חובת הרשות המקומית כמפורט בהנחייה המלאה[7] להקפיד כאשר מדובר בפונקציות מיוחדות של מצלמות מעקב ובמיזמים הכוללים: טכנולוגיות זיהוי פנים ודפוסי הליכה, טכנולוגיות ניתוח תנועה ושפת גוף, צילום תרמי/אינפרא-רד, טכנולוגיות תיוג צילומים מתוחכמות ו/או הצלבה עם מאגרים נוספים. טכנולוגיות אלה מסוגלות להפיק מידע הנחשב לבעל פוטנציאל סיכון גבוה לפרטיותם של תושבי העיר.**

4. **יידוע הציבור על הצבת המצלמות** – סעיפו הראשון של חוק הגנת הפרטיות, המציין כי חל איסור על פגיעה בפרטיותו של אדם מבלי לקבל את אישורו, וכן דרישת השקיפות בסעיף 11 לחוק, **מחייבים את הרשות המקומית ליידע את הציבור בעת הצבת מצלמות מעקב**. אמצעי היידוע המינימלי לו מחויבת הרשות המקומית הוא **הצבת שילוט קריא וברור בסמוך למקום בו מותקנת המצלמה, בדגש על מקום הכניסה לאזור הכיסוי. כמו כן, ראוי כי הרשות המקומית תפרסם באתר האינטרנט שלה מיפוי מלא של פריסת המצלמות**.

5. **זכות העיון – חובת הרשות המקומית לאפשר לאנשים שעליהם נאסף מידע לעיין במידע זה**, זאת תחת תנאים ספציפיים המוסדרים בסעיף 13 לחוק ובתקנות הגנת הפרטיות. הקלטות המצלמות מהוות גם הן מאגר מידע עליו חלה זכות העיון, אולם במימוש זכות העיון במאגר צילומים **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.

6. **אבטחת המידע הנאסף** – בהמשך לאמור בחלקים הקודמים של מדריך זה, סעיף 17 לחוק הגנת הפרטיות מטיל אחריות לאבטחת המידע על בעל המאגר, מנהלו ומחזיקו. בתוך כך, **מחובת הרשות המקומית לוודא קיום אמצעי האבטחה המפורטים בתקנות הגנת הפרטיות (אבטחת מידע)**[8].

---

7 | ראו הנחיית רשם מאגרי המידע מס' 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן" באתר הרשות להגנת הפרטיות.

8 | מידע נוסף ניתן למצוא באתר הרשות להגנת הפרטיות ובמדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע).

דוגמה

ברשות מקומית מסוימת הוחלט על הצבת מצלמות בחופי הים שבתחומה למטרה אחת ויחידה – שמירה על שלום הציבור ומניעת פגיעה ואלימות. לאור זאת, נקבעה רזולוציית צילום גבוהה משום שייתכן שיהיה צורך לזהות את פניהם של המבקרים בחוף.

כעת, מעוניינת העירייה לעשות שימוש בצילומי המצלמות לצרכי קמפיין תיירותי.

לאור העובדה שהשימוש בצילומים למטרות עידוד תיירות לא הוגדרה כתכלית הצבת המצלמות בחופים, חל איסור להשתמש בצילומים למטרה זו.

אם מבקשת הרשות המקומית להשתמש בצילומים למטרות תיירות, עליה להגדיר זאת מראש, להקפיד על 'תכנון לפרטיות' ולוודא, בין השאר, שימוש ברזולוציית צילום נמוכה יותר.

תחבורה במרחב העירוני

מגמת נוכחות הרשויות המקומיות בחיי התושבים הולכת וגוברת. ההשפעה של הרשות המקומית על התושב בעידן הדיגיטלי מתחזקת ואחת ההשלכות המרכזיות היא על תחום 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 המיושב יאפשר את שיפור השירות, התייעלות כלכלית וניצול נכון של משאבים.

התחבורה בעידן הדיגיטלי מתפתחת במהירות על ידי ענקיות טכנולוגיה בינלאומיות ועל ידי חברות ההזנק המקומיות 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 ביתר, 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 מדובר על שימוש בנתונים הכוללים מידע אישי של התושבים 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 התושב.

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

פרק זה מגדיר את האופן שבו רואה הרשות את תכולת תחום התחבורה בעיר החכמה, מנתח את הסיכונים האפשריים לפרטיות, מנחה כיצד יש לנהוג בתכנון והקמה של מיזם תחבורתי חדש, וכיצד לנהוג בעת הפעלת מיזם תחבורתי קיים.

תחבורה במרחב העירוני

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 ופוטנציאליות נכון לרגע כתיבת המדריך ונועדה לסייע לעובדי הרשות המקומית לערוך ניתוח של מיזם קיים או עתידי בראי הסיכונים לפרטיות התושבים.

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 עבור תשלום.	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 מבוסס 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 ו\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. אולי כדאי להתייחס גם לאפשרות להנפיק כרטיסים אנונימיים כמו שקיים ברב-קו
	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 סלולרי.
ניטור ובקרת תנועה	ניטור ומעקב תנועה בזמן אמת	בקרה על עומסי תנועה ברחבי הרשות המקומית על ידי רשת מצלמות וחיישנים המחוברים למרכז בקרה המספק תמונת מצב מקיפה.	סיכון תלוי במאפייני רשת המצלמות – סיכון גבוה ברזולוציה גבוהה ויכולת זיהוי פרטי רכב וזיהוי פנים. סיכון נמוך אם מבוצע זיהוי עומס תנועה בלבד.

תחום	תת תחום	פירוט	רמת הסיכון לפגיעה בפרטיות
ניטור ובקרת תנועה	**מערכות בקרת רמזורים ואופטימיזצית תנועה**	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.
	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	ניטור מקומות חניה פנויים ברחבי רשות או חניונים והכוונה בהתאם על ידי שילוט אלקטרוני או ממשק באפליקציה תואמת.	סיכון תלוי בסוג החיישן –אם מבוסס מצלמות ושמירת מאגר הצילום, סיכון גבוה לפרטיות. אם מבוסס חיישן תנועה – אין סיכון לפרטיות.
	חניה שיתופית	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 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, 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. במסגרת כך, 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. את המערכת ואת שירותי הפעלתה תספק חברה חיצונית שתזכה במכרז שתוציא 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 התושבים. התסקיר יסייע לבחור ב**אלטרנטיבה 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 הרשות להגנת הפרטיות. הבקשה 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 תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד. מומלץ, כי בקרה תבוצע על ידי **האחראי על תחום הפרטיות** המוגדר ברשות המקומית.

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 להנחיות הרשות להגנת הפרטיות ולהוראות תקנות הגנת הפרטיות (אבטחת מידע) בנושא מיקור חוץ.

הפעלה ומימוש:

על מנת **לצמצם פגיעה בפרטיות** תושבים או עוברי אורח אשר עשויים להיות מצולמים, מוצע כי מצלמות המערכת יופנו לכביש ולא יצלמו את המדרכות, לרבות צילום מעברי חציה, ולא יתעדו כניסות לבתים ובתי עסק. מעבר לכך, איכות התמונה תהיה ברזולוציה נמוכה על מנת שלא ניתן יהיה לזהות פנים אך חדה מספיק בכדי להבחין בתנועת הרכבים ובהולכי רגל.

מערכת המידע תשמור את הנתונים במשך 24 שעות על מנת שיהיה ניתן להוציא ממנה בזמן אמת קטעים עבור תחקור ובדיקת מידע, ולאחר מכן המידע ימחק. 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

מאגר המידע של המערכת יהיה נפרד ממאגרים אחרים ברשות המקומית, והגישה 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.

תיק נתוני תושב

למען הסר ספק, המדריך כולו וגם דף מידע זה מפורסם לצורך הנוחות בלבד ואין הוא ממצה את החובות הנדרשות בחוק, בתקנות ובהנחיות הרשות. במקרה של סתירה יגברו הוראות החקיקה והתקנות.

רשות מקומית מנהלת מאגרי מידע שונים, המכילים נתונים שונים ומידע רב אודות תושביה. פרק זה מתמקד במאגרי מידע המכילים מידע אישי אודות תושבי הרשויות המקומיות, ובפרט ב"תיק נתוני תושב".

תיק נתוני תושב הוא מאגר מידע שבבעלות הרשות המקומית ומכיל מידע אישי אודות תושבי הרשות המקומית בתחומים שונים כגון רווחה, חינוך, תשלום מיסי ארנונה ושירותים דיגיטליים נוספים.

תיק נתוני התושב מבקש לתכלל את מלוא המידע הקיים ברשות אודות התושב, מתוך מטרה להקל ולייעל את עבודת השירות, לספק תשתית שירותים מתקדמים לתושבים ובמקרים מסוימים אף לבצע ניתוח סטטיסטי לשם ניהול מיטבי של עבודת הרשות.

תיק נתוני תושב יכול להיות מנוהל על ידי הרשות המקומית באופן ישיר או על ידי חברה חיצונית המספקת שירותים לרשות בתחום זה.

דף מידע זה מיועד למנמ"ר, למחלקה המשפטית, לאחראי אבטחת המידע וכל גורם שמבצע שימוש במאגר מידע או במערכת המוציאה נתונים ממאגר מידע אודות תושבים.

מונחים

הסכמה – הסכמה מדעת, במפורש או מכללא
נושא המידע – האדם שאודותיו נאסף המידע, התושב
מנהל מאגר – מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה

צמידות מטרה ואיסור העברת מידע

בעירייה מאגרים רבים למטרות שונות. חובת השקיפות בעת פניה לקבלת מידע מתושב מחייבת את הרשות המקומית להודיע לתושב אם חלה עליו חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, ואז, על הרשות להודיע זאת באופן ברור. כמו כן, על הרשות המקומית להודיע לתושב מהי המטרה לשמה מבוקש המידע וכן למי יימסר המידע ולאלו מטרות.

בשלב הבא, קבלת המידע מחייבת שמירה על עקרון צמידות המטרה, לפיו אין לעשות שימוש במידע שלא למטרה שלשמה נמסר.

- **מסירת מידע מאת גוף ציבורי**

אסורה במידה ו-

- לא מתקיים אחד מן החריגים המפורטים בפרק ד' לחוק הגנת הפרטיות. למשל – המידע פורסם לרבים על פי סמכות כדין, או שהועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה.
- המידע התקבל בתנאי שלא יימסר לאחר.

דוגמאות

1. מותרת העברת נתונים סטטיסטיים מהרשות המקומית ללמ"ס, לפי הסמכות המפורשת שנקבעה בפקודת הסטטיסטיקה.
2. אסורה העברת נתונים אודות תושבים ללשכת שר, אם הדבר מנוגד למטרת קבלת הנתונים המקורית.

- **בקשת אישור להעברת מידע** - במידה ועולה צורך להעברת מידע בין מאגר עם מטרה מוגדרת למאגר אחר, פנימי לרשות או לגוף ציבורי אחר, או לבעל תפקיד אחר שאינו מורשה, אשר אינה עומדת בחריג המפורט בפרק ד' לחוק הגנת הפרטיות – **אסור להעביר את המידע ללא הסכמה של נושא המידע**, וגם לאחר קבלת הסכמה אין להעביר מידע או לעשות בו שימוש הפוגע בפרטיות במידה העולה על הנדרש.

דוגמאות

1. אסורה העברת נתונים, הכוללים רשימת תושבים ופרטי יצירת קשר לסגן ראש עיר, גם אם ממונה על האגף הנידון, אם אין הנתונים נדרשים על מנת שיבצע את עבודתו.
2. בעת רישום לגני ילדים, ועל מנת למנוע הליך ביורוקרטי מורכב וחוזר, מעוניינת העירייה להתשמש בנתוני תושבים ממאגר תשלום הארנונה בעיר כדי שלא ידרשו לספק טפסים פעם נוספת. הליך זה יתאפשר רק במידה ובעת הרישום התושב יאשר באופן מודע את העברת המידע בין המאגרים.

מאגר מידע

- **זכות עיון במידע** - כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.
- **הרשאות - ההנחיות אודות ההרשאות נגזרות מהתקנות שנקבעו בחוק.**
  - יש לקבוע הרשאות גישה למאגר, בין אם ישירות למאגר או למערכת מידע השואבת נתונים ממאגר, לכל עובד במידה הנדרשת לו לביצוע תפקידו.
  - יש לנהל רשימת הרשאות מעודכנת.
  - **הרשאות צולבות** - נדרשת בקרה ומיפוי ההרשאות הניתנות לעובדי הרשות על מנת לצמצם ולהגביל הרשאות למספר מאגרים המכילים נתונים הניתנים להצלבה שיאפשרו גיבוש תמונה מלאה אודות תושבים, שעלולה להוביל לשימוש בנתונים שלא למטרה שלשמה נמסרו.
  - העיריה מחויבת לוודא שמי שניגש למאגר הוא אכן עובד מורשה, וזאת באמצעות זיהוי ואימות לפחות כנדרש בתקנות אבטחת המידע. כמו כן, נדרש לנהל מנגנון המתעד באופן אוטומטי ועצמאי כל גישה למערכת.
- **תיקון פרטים** - אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ – למחזיק מאגר המידע, בבקשה לתקן את המידע או למוחקו.
- **אחריות בנושא המאגר** – בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע, וכן ממונה אבטחת המידע כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.
- **ביקורת תקופתית**
  - אחת ל-24 חודשים לפחות יש לערוך ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, על מנת לוודא עמידתו בהוראות התקנות.
  - בדו"ח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.
  - הנהלת הרשות המקומית תדון בדו"חות הביקורת שיועברו לו, ותבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

דוגמה

- בסיום כל שנה, מקיימת רשות מקומית ביקורת פנימית על ידי עובד שהוכשר לעניין ואינו ממונה אבטחת מידע בשגרה.
- במהלך הביקורת, יבחן המבקר את אמצעי האבטחה, מיפוי הרשאות למאגרים והרשאות בפועל, הצלבות של הרשאות קיימות ועבודה עם גורמים חיצוניים.
- במסגרת הביקורת, יבצע בדיקה גם בקרב קבלנים חיצוניים העובדים עם הרשות ולהם גישה למאגרי מידע מתוקף ההתקשרות עימם.
- בסיום הביקורת, יציג להנהלת הרשות דוח ממצאים והמלצות לדרכי פעולה לפתרון ליקויים.

התקשרות חיצונית עם ספקים

בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), ולהנחיות רשם מאגרי המידע בנוגע לשימוש בשירותי מיקור חוץ, מתן גישה לגורם חיצוני יוצרת סיכונים מיוחדים, ולכן מצריכה בחינה של הסיכונים הכרוכים, ועמידה בהנחיות התקשרות.

אחריות -

- בהתקשרות מול גורם חיצוני, החובות והאחריות המלאה על מאגר המידע, הנתונים בו, ההגנה על הפרטיות ואבטחת המידע הם של הרשות המקומית – **בעלת המאגר**.
- על בעל המאגר ומנהל המאגר ממשיכות לחול החובות והאחריות כאילו הוא מבצע את הפעילות בעצמו.
- טרם הוצאת פעילות למיקור חוץ, על הרשות לבחון האם היא רשאית להוציא את המידע אל מחוץ לשליטתה, בהתאם למגבלות חוקיות ואתיות. אם אין מגבלה פורמלית, מומלץ לקיים הליך בחינה האם ראוי, לאור אופי המידע, להעביר את המידע או את עיבודו לגורם חיצוני.
- טרם בחירת הקבלן מספק השירות, יבחנו ניסיון הקבלן בעיבוד מידע אישי, רקע ומוניטין הקבלן וקיום חשש לניגוד עניינים או סיכון אחר לשימוש פסול במידע על ידי הקבלן או מי מטעמו.
- ככלל, כל הנחיה ותקנה שחלות על הרשות המקומית, חלות על קבלן חיצוני שבא בהסכם עימה בנוגע למאגרי מידע ונתונים אודות תושבים שהתקבלו מהרשות.

הגדרות להסכם מול גורם חיצוני -

- צמידות מטרה - הגדרת המטרה המפורשת לשמה מבוצעת ההתקשרות.
הגדרה ברורה להדרכת הקבלן את עובדיו ומי מטעמו בנוגע למטרה הברורה
- סוג עיבוד המידע אותו רשאי הקבלן לבצע.
- מערכות ומאגרי מידע אליהם רשאי הקבלן לגשת.
ככלל, יש לצמצם הרשאות ולהימנע מגישה בלתי מוגבלת למאגרי מידע למינימום הנדרש על מנת לספק שירות.
- המידע שיועבר לגורם החיצוני או שתינתן לו גישה אליו.
- משך ההתקשרות ואופן השבת המידע בסיום ההתקשרות או מחיקתו.
- איסור העברת מידע לצד שלישי או להשתמש במידע אליו נחשף הקבלן במהלך ההתקשרות לכל מטרה שאינה המטרה המוגדרת בהתקשרות.
- אופן יישום תקנות אבטחת המידע.
- חובת החתמה של בעלי הרשאות בקרב הגורם החיצוני על התחייבות לשמירה על סודיות המידע ועמידה בכל הגדרות דף המידע.
- במידה ובעל המאגר מתיר לגורם חיצוני (הספק) לתת שירות באמצעות גורם חיצוני נוסף (קבלן משנה), חובת הספק החותם על ההסכם לכלול בהסכם את הגורם הנוסף.
- חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- קיום האפשרות לביצוע פיקוח, בקרה ומעקב על ידי הרשות המקומית בהתאם להוראות התקנות והנחיות הרשות.

בקרה ופיקוח -

- יש לנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות, בהיקף הנדרש ובשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.
- יש לקיים ביקורות כפי שמצויין בסעיף מאגר מידע: ביקורת תקופתית, גם לגורם חיצוני שנמצא בהסכם מול הרשות.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

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

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