משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב רשויות מקומיות

כסלו תשפ"א
נובמבר 2021

1. תוכן עניינים

2. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות ("**הרשות**") מופקד על עריכת פיקוחי רוחב מגזריים או נושאיים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א-1981 ("**חוק הגנת הפרטיות**" או "**החוק**") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("**תקנות אבטחת מידע**"), במטרה לאתר הפרות של החוק, לשם הגברת מודעות המשק להוראות החוק, הגברת האכיפה היזומה של הרשות, לאיתור כשלים ענפיים הדורשים התייחסות והבהרות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות החוק.

2.1. מגזר רשויות מקומיות

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נקבע מגזר רשויות מקומיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים, זאת בשל מאפייניו הייחודיים. מאפיינים אלה כוללים, בין היתר, את העובדה שרשות מקומית הינה גוף ציבורי הכפוף להוראות חוק ייחודיות ואת יחסי האמון בין הרשות המקומית לתושב. פעילות הרשויות המקומיות אף כוללת סיכונים לפרטיות הנובעים מניהול והחזקת מידע רחב היקף ורגיש אודות תושביהן ובכלל זה מרשם התושבים, מצב הנכסים ובעליהם, מצב הגבייה ואכיפתה, מידע אודות תלמידים, תושבים המטופלים על ידי לשכות הרווחה, פירוט ספקי העירייה ונתונים כספיים בהתקשרות עימם ואף מידע אודות יעוץ פסיכולוגי וסוציאלי. גורמים נוספים לסיכון לפרטיות במגזר זה נובעים מעצם היותן של רשויות מקומיות בעלים של מאגרי מידע רבים הניתנים להצלבה, עובדה המגבירה את החשש שיעשו במידע הקיים ברשותם שימוש לצרכים החורגים ממטרת איסופו המקורית ; כמו גם שימוש רב בנותני שירותים חיצוניים המאפשר, במצבים מסוימים, חשיפה למידע רגיש הקיים במאגרי הרשות; היותן של רשויות מקומיות גופים ציבוריים המוסרים ומקבלים דרך קבע מידע אישי של תושבים מגופים אחרים; מנגנוני מחשוב גדולים שעשויים לייצר גישה למידע למספר רב של מורשי גישה, וכן נוכח פרסומי עבר של דוחות מבקר המדינה מהשנים 2012, 2017 ו-2020 אשר בחנו היבטים שונים בתחום מערכות המידע וכללו בין היתר הערות לגבי מידת העמידה של רשויות מקומיות בהוראות חוק הגנת הפרטיות ותקנותיו.

בנוסף, היבטי הפרטיות במגזר הרשויות המקומיות מקבלים חשיבות נוספת על רקע החלטת הממשלה מס' 2733 מיום 11.6.2017 אשר קבעה יעד לפיו כל רשות מקומית בישראל תהיה חכמה ובעלת תשתיות לפלטפורמות דיגיטליות. היבטים אלו באו לידי ביטוי גם במדריך הגנת הפרטיות לעיר החכמה שפרסמה הרשות להגנת הפרטיות, המתייחס בין היתר להיבטי הפרטיות שחלקן נבחנו בפיקוח רוחב זה.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותן רשויות מקומיות לעמוד בדרישות החוק והתקנות ביתר שאת, תוך הגנה על פרטיות התושבים, לרבות קיום חובות אבטחת המידע, קיום חובת השקיפות כלפי התושבים, התקשרות תקינה מול מי שמחזיק במידע במיקור חוץ, ניהול תקין של העברות מידע בין גופים ציבוריים, שימוש במצלמות מעקב במרחב הציבורי, וקיום בקרה ארגונית.

פיקוח הרוחב התמקד בעיקר באופן ניהול המידע ברשויות בנושאי גבייה, חינוך ומצלמות מעקב.

2.2. תהליך העבודה

במטרה לפעול באופן המיטבי ביותר למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות מקיימת סקרי סיכונים שמבוססים על הערכות מצב עיתיות, ונוקטת בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש בפעולותיה על המשק, על מנת לעמוד במכלול האתגרים.

תוצר הערכת המצב כולל תופעות ומגזרים הכוללים סיכונים מיוחדים לפרטיות, וממקד את תחומי העיסוק העתידיים של הרשות ואת תשתית תכנית העבודה. מגזר הרשויות המקומיות כאמור כולל מידע רגיש בהיקף גדול ביחס לכלל תושבי מדינת ישראל, והוגדר כאחד מהיעדים בהם תמקד הרשות פעילותה.

על רקע זה, פרסמה הרשות להגנת הפרטיות את 'מדריך הגנת הפרטיות לעיר החכמה' בחודש דצמבר 2018. מדריך זה עודכן ופורסם שוב בינואר 2020.

פעילות פיקוח הרוחב של הרשות כללה בחינה של יישום חוק הגנת הפרטיות ותקנותיו, במטרה לבחון ולסייע לרשויות המקומיות במימוש אחריותן לשמירה על פרטיות התושבים, תוך בחינת כמות והיקף המידע במגזר, רמת רגישות המידע, היקף המידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

בהליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל-70 רשויות מקומיות המנהלות מידע אישי על למעלה מ-5,000,000 תושבים - 33 רשויות גדולות הכוללות למעלה מ-42,000 תושבים, 10 רשויות בינוניות הכוללות בין 30,000 ל-42,000 תושבים ו-27 רשויות קטנות יותר, הכוללות בין 3,000 ל-30,000 תושבים.

שאלוני הביקורת בחנו חמישה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע לרבות שימוש במצלמות מעקב במרחב הציבורי, אבטחת מידע, העברת מידע בין גופים ציבוריים ועיבוד מידע במיקור חוץ. רמת העמידה נקבעה בהתאם למענה ולמסמכים שסופקו, לאחר שאלו נבחנו על ידי הרשות, בהתאם לרמת עמידתה של כל רשות בהוראות חוק הגנת הפרטיות והתקנות מכוחו.

2.3. ליקויים, מסקנות והמלצות עיקריות

בקרה ארגונית - נמצאה רמת עמידה בינונית-נמוכה בכל הקשור בבקרה ארגונית, שבאה לידי ביטוי בעיקר באי מינוי ממונה אבטחת מידע או במינוי שאינו עומד בהוראות התקנות בדבר עצמאותו ואי תלותו של ממונה אבטחת המידע. כמו כן, נמצאו נהלי אבטחת מידע שאינם עומדים באופן מלא בדרישות החוק, אי עריכת סקרי סיכונים וביקורות תקופתיות בנושא אבטחת מידע, הליך מיון עובדים שאינו בהתאם לדרישות התקנות והיעדר תכנית עבודה שנתית לבקרה שוטפת בתחום אבטחת המידע והגנת הפרטיות.

העברת מידע בין גופים ציבוריים - נמצאה רמת עמידה בינונית-נמוכה בכל הקשור להעברת מידע בין גופים ציבוריים, החל מהיעדר ועדה לטיפול בהעברת מידע בין גופים ציבוריים וכלה באי רישום או רישום בלתי נאות של מידע שנמסר או מתקבל מגופים ציבוריים אחרים.

ניהול מאגרי מידע - נמצאה רמת עמידה בינונית-נמוכה בכל הקשור בניהול מאגרי מידע, כאשר הכשלים העיקריים נבעו מטיפול בלתי נאות בתהליך איסוף המידע והיעדר אפשרות לתושבי הרשות המקומית לעיין במידע אודותיהם או לתקנו. כמו כן, נמצא כי לא מיושמות בקרות לבדיקת הנאותות בהתקשרות עם גורם חיצוני לשם קבלת שירותי עיבוד המידע. עוד נמצא כי, ברשויות רבות מנהל מאגר המידע שמונה לא מונה על ידי מנהל הארגון ו/או לא נרשם בפנקסי הרשות ו/או כתב המינוי אינו כולל את כלל הפרטים הנדרשים בכתב המינוי.

אבטחת מידע - מפיקוח הרוחב עולה גם כי בנושא אבטחת מידע נמצאה רמת עמידה בינונית-נמוכה ברשויות המקומיות. בין היתר, נמצא כי לא מיושמת באופן מלא מדיניות אשר תואמת את דרישות החוק והתקנות בכל הקשור לנושאי אבטחת מידע. נמצאו מקרים בהם לא בא לידי ביטוי השימוש באמצעי פיזי הנתון לשליטתו של בעל המאגר, אי עמידה במדיניות הסיסמאות ואי ביצוע סקרי סיכונים ומבדקי חדירה בהתאם לדרישת התקנות. נמצאו ליקויים בהיעדר בקרות לזיהוי משתמשים ולניהול הרשאות בהתאם לצורך לדעת, והיעדר תיעוד של אירוע אבטחת מידע. כמו כן, בכל הקשור למאגרי מידע של מצלמות מעקב במרחב הציבורי, נמצא כי רשויות רבות אינן מקפידות על אופן יידוע הציבור בדבר המצלמות, אי קביעת מורשי גישה, קיום נהלים ברורים לשימוש וכיוצא באלה.

מיקור חוץ - בקריטריון זה נמצא כי במרבית הרשויות המקומיות בהן נמצאה רמת עמידה בינונית ונמוכה, לא בוצעו כלל הפעולות הנדרשות בהתאם לתקנה 15 ולהנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי לרשות המקומית, ולא ננקטו פעולות בכדי לוודא שהגורם החיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש. בין היתר בליקוי זה לא מולאו הסכמים עם כלל הספקים, או שההסכמים נעדרים סעיפים הנדרשים על פי הסעיף בתקנות.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 69 רשויות מתוך 70 הרשויות שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלן. רשות אחת הועברה להמשך טיפול אכיפתי, וב-24 רשויות מקומיות בוצעו ביקורות מעקב לבדיקת יישום תכנית העבודה ותיקון הליקויים ובחינת העמידה בלוחות הזמנים שנקצבו לכך. על רקע הכשלים שנמצאו, דו"ח זה כולל ריכוז של ההנחיות העיקריות לתיקון הליקויים שנשלחו לרשויות המקומיות.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

ממצאי הליך פיקוח רוחב
בקרב מגזר רשויות מקומיות

אתגרים ומאפיינים ייחודיים של מגזר רשויות מקומיות

רשויות מקומיות מחזיקות מידע רב ורגיש במיוחד על תושביהם, בהיקפים עצומים על כלל תושבי מדינה ישראל.

השירותים המסופקים על ידי רשויות מקומיות הינם שירותים חיוניים והן נתפסות בעיני תושביהן כגוף אמין שאמור גם להגן עליהם, ולכן אינו נמנע ממסירת מידע רחב ורגיש.

הרשויות מסתמכות על שירותים חיצוניים במידה רבה, דבר אשר מסכן את המידע השמור במאגרים אלו במידה ואינו נשמר בהתאם לחוקים ולתקנות.

התהליך שבוצע במספרים

הליך פיקוח הרוחב התמקד בניהול מידע בעיקר בנושאים:


מצלמות אבטחה

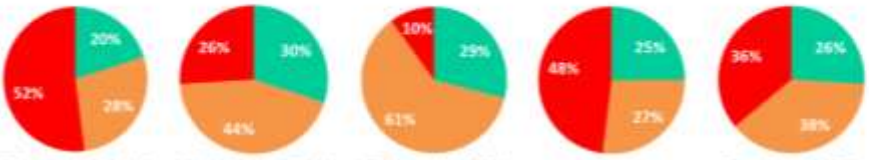

חינוך


גבייה

ממצאים – ליקויים מרכזיים:

ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר

- רמת עמידה גבוהה
- רמת עמידה בינונית/חלקית
- רמת עמידה נמוכה



ממצאי עמידה בהוראות הדין מבט השוואתי

- במאגרים בעלי רמת אבטחה גבוהה, יש לבצע מבדקי חדירה אחת ל- 18 חודשים, בהתאם לתקנה 5 (ד) לתקנות אבטחת מידע, ולוודא כי תיעוד של אירועי אבטחת מידע יישמר ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות אבטחת מידע.
- יש לבנות מנגנוני הרשאות במאגרי המידע של הרשות המקומיות בהתאם לתקנות 8 ו- 9 (א) לתקנות אבטחת מידע, אשר יבטיחו הפרדת סמכויות ויאפשרו גישה למאגרים ולמידע על פי עקרון "הצורך לדעת".
- יש לבצע סקר סיכונים על ידי גורם חיצוני מקצועי ובלתי תלוי אחת לשנה וחצי, בחינה של הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.
- אופן הזיהוי יעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- בעת עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, יקבעו במפורש כל ההוראות המפורטות בתקנה 15(א)(2) לתקנות אבטחת מידע, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- יש לפעול על-פי הקווים המנחים וכלי העזר המופיעים בהנחיית רשם מאגרי מידע מספר 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.
- על הרשויות המקומיות ליישם את דרישות החוק המתוארות בהנחית רשם מאגרי מידע מס' 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן" בכל הנוגע לאופן קבלת ההחלטה על הצבתן וההשלכות על זכויות הציבור, מיקום התקנת המצלמות, זמני הצילום, הרזולוציה, יידוע הציבור בדבר הצבת המצלמות, אופן שמירת המידע המצולם ומחיקתו, זכות העיון של המצולם במידע, אופן אבטחת המידע הנאגר ממצלמות המעקב והגבלת השימוש במידע למטרה לשמה הוצבו המצלמות.
- יש למסור הודעה לתושב בעת איסוף המידע, על נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע, ולמי יימסר המידע ומטרות המסירה.
- יש לאפשר לכל תושב לעיין במידע על אודותיו, ולתקן את המידע שעליו המוחזק במאגר המידע, אם נמצא מצא כי המידע אינו נכון, שלם, ברור או מעודכן.
- מיפוי ורישום כלל מאגרי המידע בפנקס המאגרים בהתאם להוראות החוק הכולל בין היתר רישום זהות מנהל המאגר בפנקס מאגרי המידע.
- גוף ציבורי המוסר דרך קבע מידע בהתאם לסעיף 23ג יפרט עובדה זו, ויקיים רישום של המידע שנמסר.
- יש להקים ועדה מקצועית לנושא העברת מידע בין גופים ציבוריים כנדרש בתקנות.
- יש לוודא כי הוועדה להעברת מידע בין גופים ציבוריים התכנסה לצורך דיון בניהול מידע ואבטחתו.
- יש למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכיר הכפוף ישירות למנהל המאגר.
- יש להכין נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4, לבחון את הצורך בעדכון מדיניות אבטחת המידע ולעדכנה בהתאם.
- יש להכין תכנית עבודה בנושא אבטחת מידע והגנת הפרטיות, לרבות התייחסות לגורם אחראי ולחות זמנים לביצוע אשר תעמוד בדרישות תקנות אבטחת מידע (תקנה 3(3))
- יש להטמיע תהליך מיון של עובדים חדשים שיבחן היבטים הרלבנטיים לפרטיות ולאבטחת מידע.

3. רשויות מקומיות - תמונת מצב

3.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים ספטמבר 2019 למאי 2020 במגזר הרשויות המקומיות.

3.2. רקע על המגזר

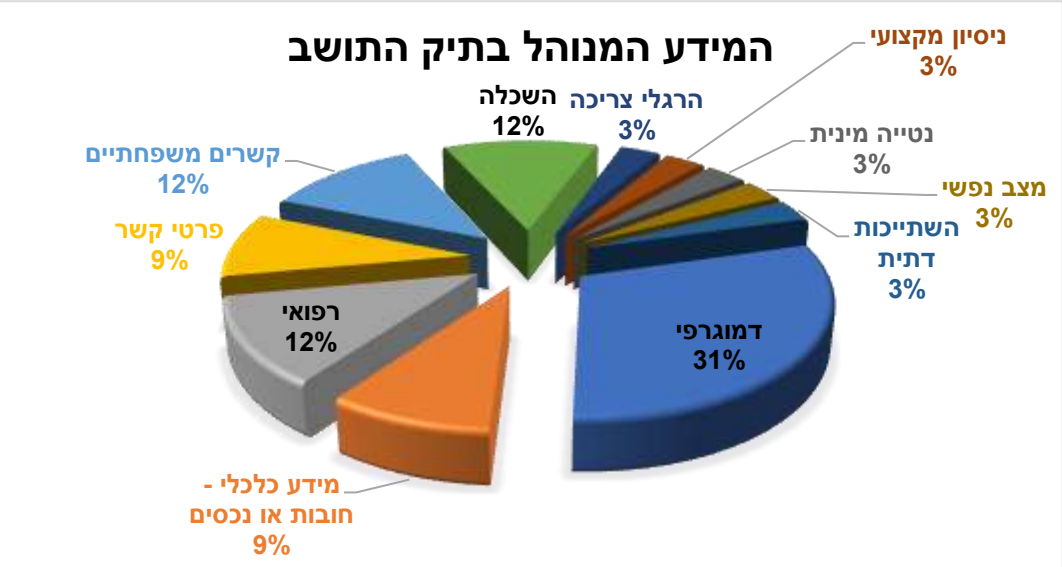
במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נקבע מגזר רשויות מקומיות[1] בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים, בשל מאפייניו הייחודיים, ובין היתר, בשל היותה של רשות מקומית גוף ציבורי הכפוף להוראות חוק ייחודיות ולאור יחסי האמון בין הרשות המקומית לתושב. פעילות הרשויות המקומיות, כוללת סיכונים לפרטיות הבאים לידי ביטוי, בין היתר, בניהול והחזקת מידע רחב ורגיש אודות תושבי הרשות המקומית ובכלל זה מרשם התושבים, מצב נכסים ובעליהם, מצב הגבייה ואכיפתה, מידע אודות תלמידים, רישום ושיבוץ תלמידים, זכאות לבגרויות, מידע אודות המשתמשים בהסעות, תלמידי חינוך מיוחד, תושבים המטופלים על ידי לשכות הרווחה, פירוט ספקי העירייה ונתונים כספיים בהתקשרות עימם ואף מידע אודות יעוץ פסיכולוגי וסוציאלי. גורמים נוספים לסיכון לפרטיות במגזר זה נובעים מעצם היותן של רשויות מקומיות בעלים של מאגרי מידע רבים הניתנים להצלבה, עובדה המגבירה את החשש שיעשו שימוש במידע הקיים ברשותן לצרכים החורגים ממטרת איסופו המקורית; כמו כן, שימוש רב בנותני שירותים חיצוניים מאפשר, במצבים מסוימים, חשיפה למידע רגיש הקיים במאגרי הרשות; היותם של רשויות מקומיות גופים ציבוריים המוסרים ומקבלים דרך קבע מידע אישי של תושבים מגופים אחרים; מנגנוני מחשוב גדולים שעשויים לייצר גישה למידע למספר רב של מורשי גישה, וכן נוכח פרסומי עבר של דוחות מבקר המדינה מהשנים 2012, 2017 ו-2020 אשר בחנו היבטים שונים בתחום מערכות המידע וכללו בין היתר הערות לגבי מידת העמידה בהוראות חוק הגנת הפרטיות ותקנותיו.

[1] הרשויות המקומיות בישראל נחלקות לארבעה סוגים: עירייה, מועצה מקומית, מועצה אזורית ומועצה מקומית תעשייתית. הליך פיקוח הרוחב אפיין את יעדי הפיקוח לפי מספר נושאי המידע (תושבים), בחלוקה של רשויות גדולות, בינוניות וקטנות כפי שיפורט בפרק תהליך העבודה שלהלן.

בנוסף, היבטי הפרטיות במגזר הרשויות המקומיות מקבלים חשיבות נוספת על רקע החלטת הממשלה מס' 2733 מיום 11.6.2017 אשר קבעה יעד לפיו כל רשות מקומית בישראל תהיה חכמה ובעלת תשתיות לפלטפורמות דיגיטליות. היבטים אלו באו לידי ביטוי גם במדריך הגנת הפרטיות לעיר החכמה שפרסמה הרשות להגנת הפרטיות, המתייחס בין היתר להיבטי הפרטיות שחלקן נבחנו בפיקוח רוחב זה.[2]

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את הרשויות המקומיות לעמוד ביתר שאת בדרישות החוק והתקנות, תוך הגנה על פרטיות התושבים, לרבות קיום חובות אבטחת המידע, קיום חובת השקיפות כלפי התושבים, התקשרות תקינה מול מי שמחזיק במידע במיקור חוץ, ניהול תקין של העברות מידע בין גופים ציבוריים, וקיום בקרה ארגונית.

נוכח כל אלה הגדירה הרשות להגנת הפרטיות מגזר זה כיעד פיקוח רוחב משמעותי, כאשר פיקוח הרוחב התמקד בעיקר באופן ניהול המידע בנושאי גבייה, חינוך ומצלמות מעקב על ידי הרשויות.



[3]

[2] מדריך הגנת הפרטיות לעיר החכמה, ינואר 2020 - https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

[3] נתוני הגרפים מתוך תשובות וממצאי הליך פיקוח הרוחב כפי שניתנו על-ידי הרשויות. המידע המוצג בגרף מתוכלל, כאשר קיים שוני בסוגי המידע בין הרשויות המקומיות השונות

3.3. תהליך העבודה

במטרה לפעול באופן המיטבי ביותר למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות מקיימת סקרי סיכונים שמבוססים על הערכות מצב עיתיות, ונוקטת בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש בפעולותיה על המשק, על מנת לעמוד במכלול האתגרים. הרשות פועלת על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, בתחומים בהם ישנה השפעה רוחבית על מגזרים שונים, הכוללים מספר רב של משתמשים ו מידע רגיש.

תוצר הערכת המצב כולל תופעות ומגזרים הכוללים סיכונים מיוחדים לפרטיות, וממקד את מוקדי העיסוק העתידיים של הרשות ואת תשתית תכנית העבודה. כאמור, מגזר הרשויות המקומיות כולל מידע רגיש בהיקף גדול, על כלל תושבי מדינת ישראל, ומשכך הוגדר כאחד מיעדיה של הרשות.

על רקע זה, פרסמה הרשות להגנת הפרטיות את 'מדריך הגנת הפרטיות לעיר החכמה' בחודש דצמבר 2018.[4] מדריך זה עודכן ופורסם שוב בינואר 2020. המדריך מרכז מידע בנושאי הגנת הפרטיות, מכיל דוגמאות לשיטות עבודה מומלצות על מנת לסייע לרשויות המקומיות ולעובדיהן לנווט בנושאים מורכבים אלה, ומסייע בהבהרת הדרך למציאת איזון נכון ברשות המקומית בין איסוף ועיבוד מידע לבין שמירה על הפרטיות והפעולות הנדרשות למען הגנה ושמירה על פרטיות התושבים ברשות המקומית.

פעילות פיקוח הרוחב של הרשות כללה בחינה של יישום חוק הגנת הפרטיות ותקנותיו, במטרה לבחון ולסייע לרשויות המקומיות במימוש אחריותן לשמירה על פרטיות התושבים, תוך בחינת כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה

[4] מדריך הגנת הפרטיות לעיר החכמה, ינואר 2020 - https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

בהליך הפיקוח פנתה הרשות בדרישה למילוי שאלון ביקורת ל-70 רשויות מקומיות המנהלות מידע אישי על למעלה מ-5,000,000 תושבים, שנבחרו על פי קריטריונים שונים על ידי הרשות. ביניהן נכללות 33 רשויות גדולות הכוללות למעלה מ-42,000 תושבים, 10 רשויות בינוניות הכוללות בין 30,000 ל-42,000 תושבים ו-27 רשויות קטנות יותר הכוללות בין 3,000 ל-30,000 תושבים.

במסגרת התהליך בוצעו תהליכים של השלמה ואימות של ידיעות ומסמכים. בסיום ההליך מתוך 70 הרשויות המפוקחות, נמצאו ב-69 מתוכן ליקויים הדורשים תיקון כאשר רשות אחת מתוך 70 הרשויות העבירה מענה חלקי בלבד, ועל כן הועברה להמשך טיפול אכיפתי במסגרת הפיקוח המנהלי במחלקת האכיפה ברשות.

בהתאם לממצאים, הנחתה הרשות את אותן רשויות מקומיות בהן נמצאו ליקויים לתקן את הליקויים שנמצאו, ולהגיש לרשות מסמך המפרט את הליקויים אשר תוקנו, והתחייבות חתומה בידי נושא משרה בכיר בארגון לתיקון יתר הליקויים על פי תכנית עבודה מסודרת של הארגון ולוחות זמנים לביצוע. הרשויות נתבקשו לתעדף את תיקון הליקויים, הן מבחינת התכנית, והן מבחינת הטיפול בפועל, על בסיס גישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בקריטריונים הבאים: עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, בקרה ארגונית והעברת מידע בין גופים ציבוריים.

כבכל שנה, מבצעת הרשות ביקורות מעקב על המגזרים שנבחנו במסגרת פיקוחי הרוחב, ובתחילת שנת 2021 הפיצה הרשות ל-24 רשויות מקומיות, המהוות 34% מסך הגופים שנבדקו, דרישת דיווח אודות יישום תכנית העבודה ותיקון הליקויים ובחינת העמידה בלוחות הזמנים שהוקצו לכך, בהתייחס לכל אחד מהליקויים שנמצאו בהליך הפיקוח בארגון. בנוסף, במסגרת פיקוחי המעקב, פנתה הרשות לגופים אשר טרם השיבו באופן מלא לדרישת תיקון הליקויים, ואלה נדרשו להעביר דו"ח עדכני מפורט אודות יישום תכנית העבודה ותיקון הליקויים בהתייחס לכל אחד מהליקויים שנמצאו בהליך פיקוח הרוחב ושפורטו במכתבי הדרישה, לרבות בהתייחס לאופן תיקון הליקוי ומועד התיקון, בהתייחס

ל-556 ליקויים שנמצאו בהליך הפיקוח בגופים בהם בוצע פיקוח המעקב. כמו כן, הוציאה הרשות דרישה לגופים שכבר העבירו את תשובתם, להעביר לה דיווח עדכני - חתום בידי נושא משרה בכיר - אודות סטטוס יישום תכנית העבודה ותיקון הליקויים. נכון למועד זה, מבין הרשויות שבוצע בהן פיקוח מעקב, למעלה מ-62% מהרשויות דיווחו כי הן מצויות בהליך או שסיימו את תיקון הליקויים שנמצאו.

הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע להליכי אכיפה משלימים אל מול רשויות אשר נבחנו בכל הנוגע למסירת תכניות העבודה והן באשר ליישומן.

3.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו

במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לקריטריונים שונים ובהם:

- **בקרה ארגונית** - קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** - קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, וכן התייחסות לשני תת קטגוריות:
  - **עיבוד מידע אישי במיקור חוץ** - לרבות בחינת ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע;
  - **ניהול מאגרי מצלמות מעקב במרחב הציבורי** - לרבות אופן היידוע והשימוש של הרשויות המקומיות במצלמות מעקב במרחב הציבורי;[5]

[5] השאלות שנשאלו בנוגע לניהול מאגרי מצלמות המעקב נשאלו בשלב זה לצורכי מחקר בנוגע לאופן יישום הנחיית רשם מאגרי מידע מס' 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן",

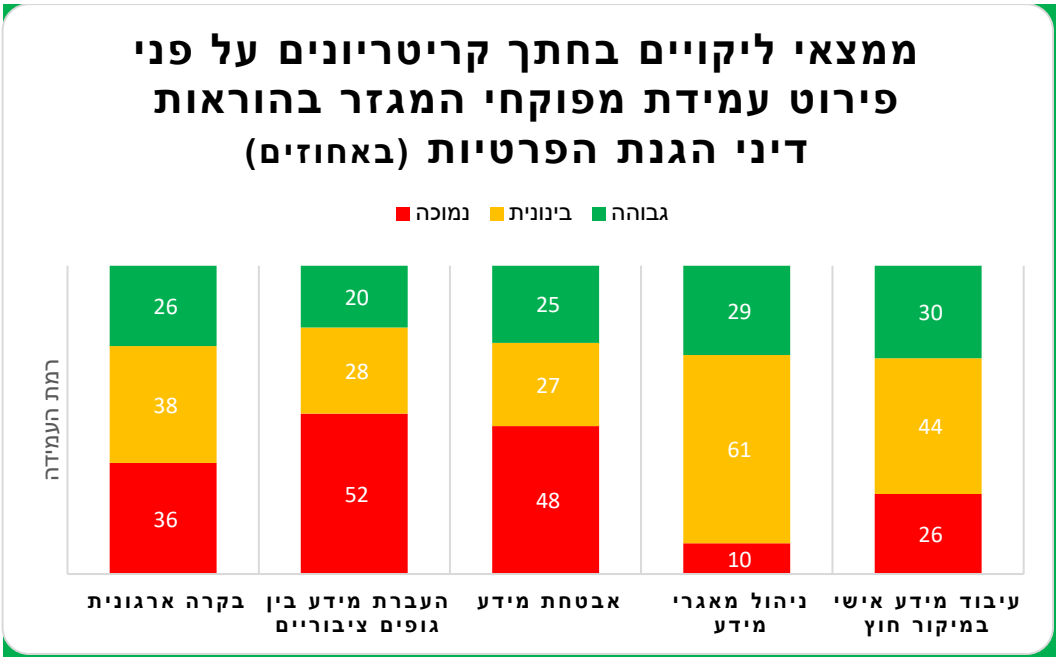
- **אבטחת מידע** - בחינת עמידת הרשויות המקומיות בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתו;
- **העברת מידע בין גופים ציבוריים** - בחינת קיומן של ועדות הבוחנות את הצורך בהעברת המידע, אי העברת מידע עודף והסמכות להעברה וקבלת מידע מגופים ציבוריים אחרים ואליהם.

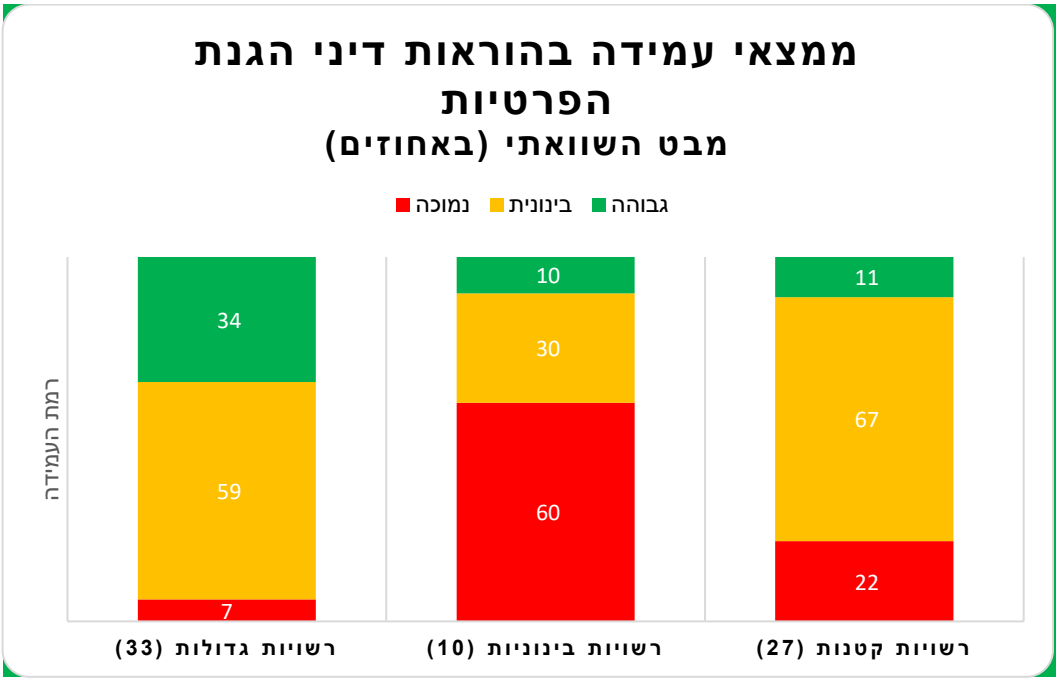
רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הרשויות המקומיות, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:

- עמידה של בין 80% - 100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;
- עמידה של בין 50% - 80% מוגדרת כרמת עמידה בינונית/חלקית;
- עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

כאשר ההמלצות לתיקון הליקויים בדו"ח זה ניתנות באופן רוחבי לכלל הרשויות המקומיות המנהלות מאגרי מצלמות מעקב.

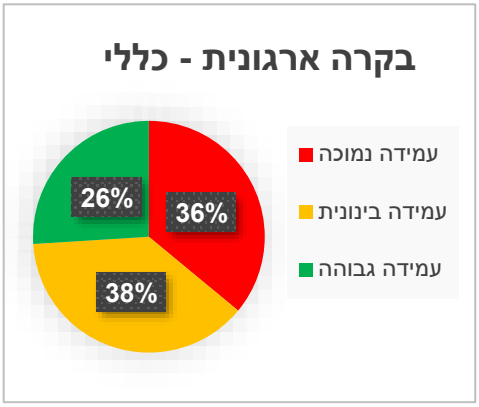
4. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי





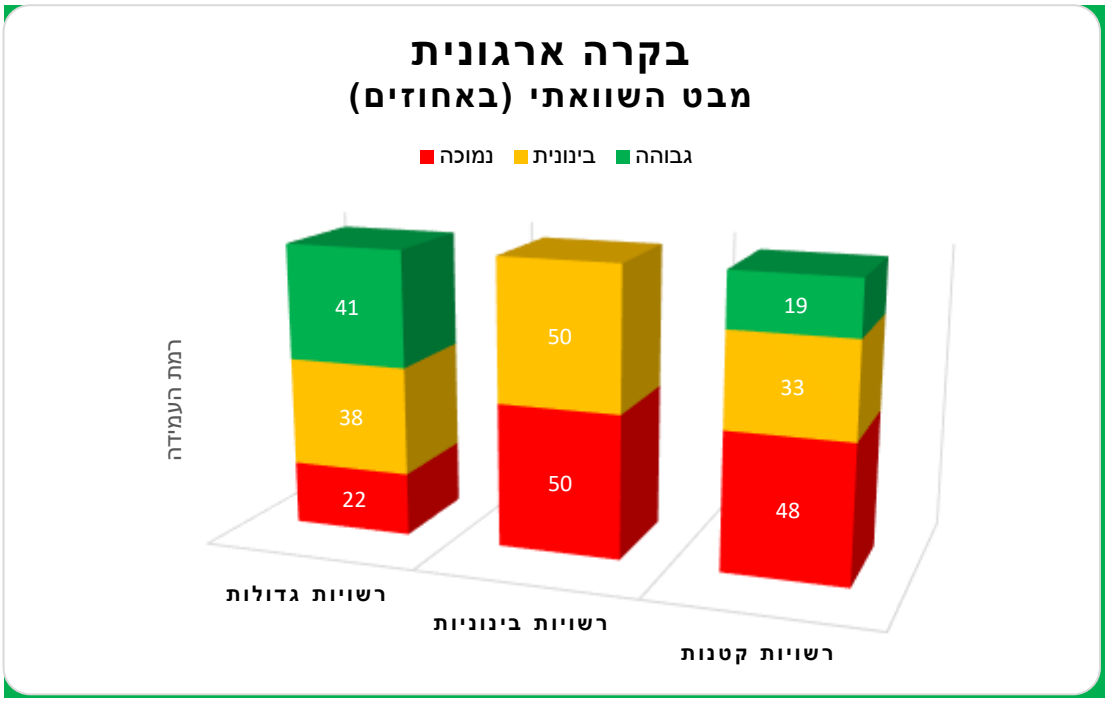
את טבלת הממצאים העיקריים שנמצאו במגזר וההנחיות שניתנו לתיקון הליקויים לרשויות המקומיות הספציפיות, ניתן למצוא בנספח א' להלן.

4.1. בקרה ארגונית



במסגרת בחינת קריטריון זה, נמצא כי רק 26% מהרשויות עמדו ברמה גבוהה בהוראות החוק בנוגע לבקרה ארגונית, בעוד ש-74% נמצאו כבעלות רמת עמידה בינונית ונמוכה בהוראות החוק כאמור.

במבט השוואתי, **עיקר הליקויים נמצאו ברשויות המקומיות הבינוניות אשר מחצית מהן נמצאו ברמת עמידה נמוכה בקריטריון זה, והמחצית השנייה נמצאו ברמת עמידה בינונית, כאשר אף רשות מקומית אשר הוגדרה כרשות בינונית לא נמצאה כממלאת את דרישות החוק והתקנות בקריטריון זה ברמה גבוהה**, קרי באופן העולה על 80% תאימות להוראות הדין. ליקויים רבים נמצאו גם ברשויות הקטנות אשר 81% מהן נמצאו ברמת עמידה בינונית ונמוכה. למעשה רמת העמידה הגבוהה ביותר בקריטריון זה נמצאה בקרב הרשויות הגדולות בהן נמצאה 41% רמת עמידה גבוהה.

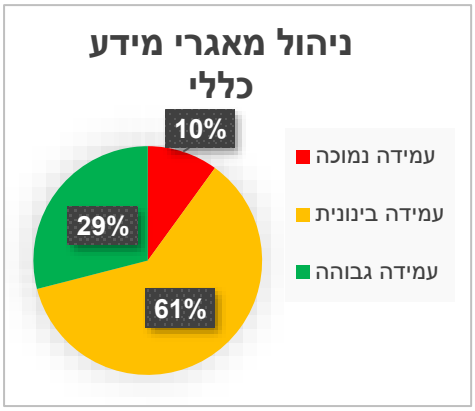


עיקר הליקויים בקריטריון זה נבעו מהסיבות שלהלן:

- מהבדיקה עלה כי נמצאו רשויות מקומיות אשר לא צרפו תיעוד לנהלי אבטחת מידע ולתכנית עבודה שנתית או שהנהלים היו חלקיים בלבד, בין היתר נמצאו נהלי אבטחת מידע הכוללים מילוי דרישות התקנות לעניין זה באופן חלקי בלבד. עוד עלה כי בחלק מהרשויות המקומיות לא מבוצעת הכנת תכנית שנתית בכל הקשור לבקרה שוטפת בנושא העמידה בדרישות החוק והתקנות.
- נמצא כי במרבית הרשויות הנמצאות ברמת עמידה נמוכה ובינונית, סקרי סיכונים וביקורות בנושא אבטחת מידע במאגרים ברמת אבטחה בינונית וגבוהה, לא נערכו כנדרש בתקנות.
- במרבית הרשויות הנמצאות ברמת עמידה נמוכה ובינונית, כתב המינוי לא תאם את דרישות רשם מאגרי המידע, ולא מונה ממונה אבטחת מידע – על אף החובה המפורשת הקבועה בחוק – או שמונה ממונה שלא על-פי התקנות, באופן בו תפקידים ותחומי אחריות היו מרוכזים אצל גורם יחיד באופן אשר עלול להעמידו בחשש לניגוד עניינים, בניגוד לדרישות הקבועות בתקנות.
- נמצא כי עובדים חדשים ברשויות המקומיות או כל גורם שמקבל גישה למאגר או למערכת המאגר אינם עוברים תהליך מיון ולא נבדקת התאמתם לקבלת הגישה למאגרי המידע, או שהליכי מיון העובדים והדרכות עובדים אינם נעשים כנדרש בחוק ובתקנות. תדירות ההדרכות פחותה מאחת לשנתיים או שההדרכות אינן כוללות את נושא אבטחת מידע והגנת הפרטיות בצורה מספקת.

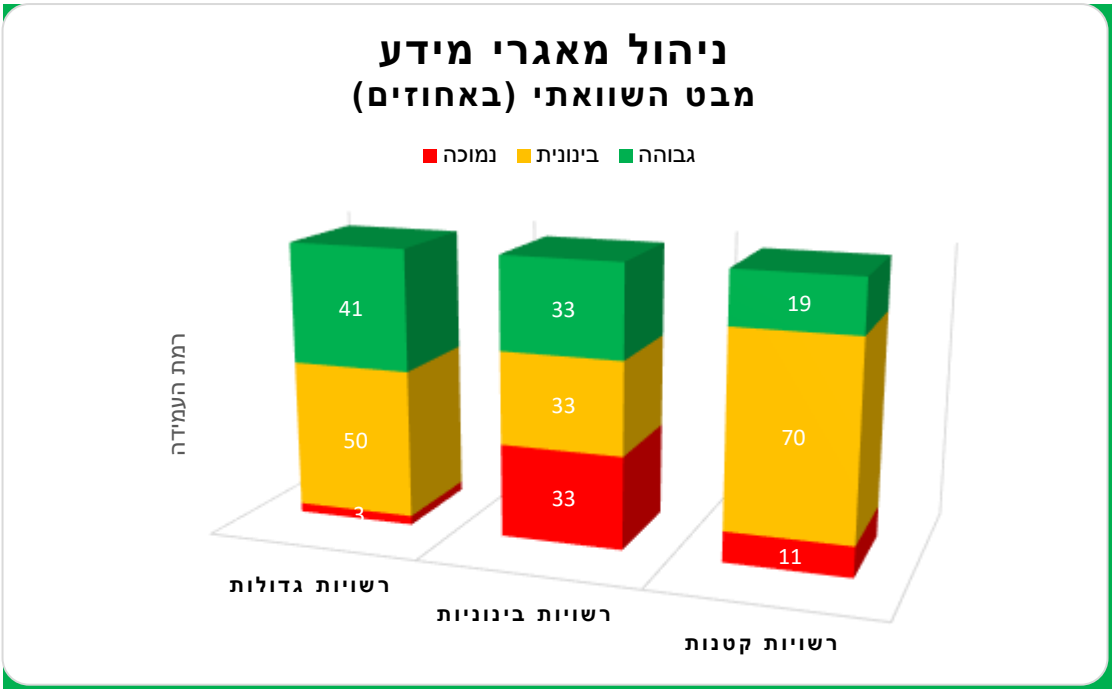
4.2. ניהול מאגרי מידע

במסגרת בחינת קריטריון זה, נמצא כי **פחות משליש (29%) מהרשויות המקומיות שנבדקו עומדות בהוראות החוק בנושא ניהול מאגרי מידע ברמת עמידה גבוהה**, בעוד שב-71% מהרשויות המקומיות נמצאה רמת עמידה בינונית-נמוכה בהוראות החוק בנושא זה.



במבט השוואתי בקריטריון זה ניתן לראות יתרון לרשויות הגדולות והבינוניות אשר הראו רמת עמידה גבוהה יחסית (41% ו-33% בהתאמה), **לעומת הרשויות הקטנות בהן נמצאה רמת עמידה גבוהה**

ב-19% מהרשויות בלבד. עם זאת, מבין הרשויות המקומיות בהן נמצאה רמת עמידה נמוכה, ניתן לראות כי דווקא בקרב הרשויות הבינוניות נמצא שיעור גבוה (33%) ברמת עמידה נמוכה בקריטריון זה בהשוואה לרשויות הגדולות והקטנות..

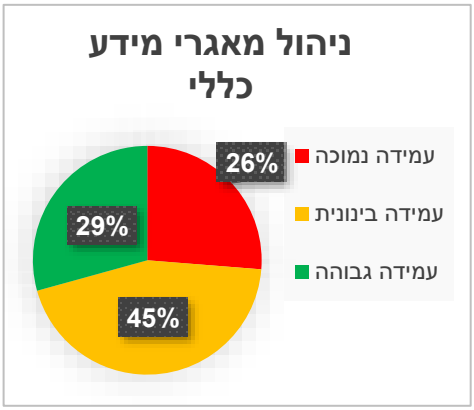


עיקר הליקויים בקריטריון זה נבעו מהסיבות שלהלן:

- בלמעלה ממחצית מהרשויות בהן נמצאה רמת עמידה בינונית ונמוכה, נמצא כי הרשויות אינן מקפידות על שקיפות בנוגע למקור הסמכות לאיסוף המידע האישי על התושבים, ואינן מקפידות על יידוע התושבים שעליהם מוחזק המידע בדבר זכויותיהם בנוגע למאגר המידע בו נשמרים פרטיהם, בהתאם לסעיף 11 לחוק, בעת פניה לקבלת מידע מהתושב.
- לא ניתנה לנושא המידע האפשרות לעיין במידע אודותיו לפי בקשתו כנדרש בסעיף 13 לחוק ואף לא האפשרות לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק.

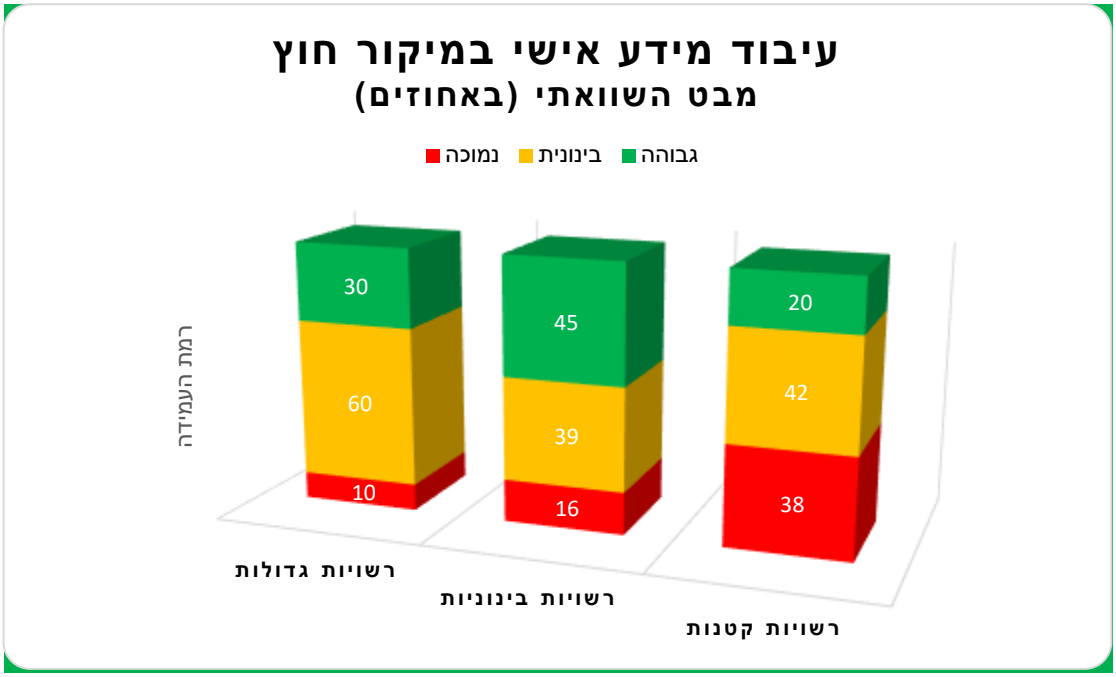
4.2.1. עיבוד מידע אישי במיקור חוץ

- במסגרת בחינת קריטריון זה, נמצא כי פחות משליש (29%) מהרשויות המקומיות שנבדקו עומדות בהוראות החוק בנושא עיבוד מידע אישי במיקור חוץ ברמת עמידה גבוהה, **בעוד שב-71% מהרשויות המקומיות נמצאה רמת עמידה בינונית-נמוכה** הבאה לידי ביטוי בין היתר באי ביצוע כלל הפעולות הנדרשות בהתאם לתקנה 15 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי לרשות המקומית, ואי נקיטת פעולות בכדי לוודא שהגורם החיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש. בין היתר לא מולאו הסכמים עם כלל הספקים, או שההסכמים נעדרים סעיפים שיש חובה לכלול על פי תקנה 15.



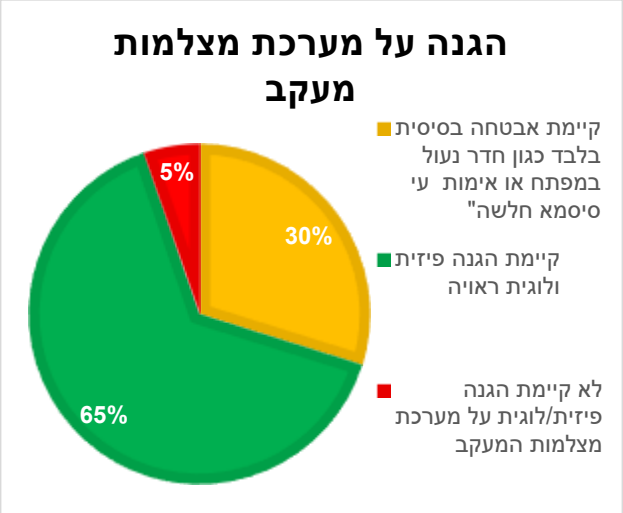
- עיקר הליקויים בקריטריון זה נבעו מהסיבות שלהלן:
  - מבין הגופים שנבדקו בקריטריון זה, עלה כי **כמעט מחצית מהגופים המבצעים עיבוד מידע אישי במיקור חוץ נמצאו ברמת עמידה בינונית ונמוכה בכל הקשור לקיום תקנה 15**. 32% מהרשויות לא קיימו הסכמים מסודרים עם ספקי מיקור החוץ אשר להם הרשאת גישה למידע, או שההסכמים לא כללו את הדרישות המפורטות בתקנה. 32% מהרשויות קיימו הסכמים עם ספקי מיקור החוץ, אך לא הקפידו לכלול בהם את כל הדרישות המפורטות בתקנה 15, ורק 52% מהרשויות הקפידו לקיים הסכמים עם ספקי מיקור החוץ, ולכלול בהם את כלל הדרישות המפורטות בתקנה.
  - מעבר לדרישות המפורטות בתקנה 15(א)-(ח), בבדיקה האם הגופים מבצעים פעולות פיקוח ובקרה על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בתקנה 15(4), נמצא כי **רק 21% מהגופים מבצעים בדיקה ממשית כדי לוודא שספק מיקור החוץ נוקט באמצעים הנדרשים בכדי**

לעמוד בהוראות. 60% מהרשויות שאלו את ספק מיקור החוץ האם הוא עומד בהוראות ההסכם והתקנות, מבלי לנקוט בפעולות כדי לוודא את נכונות האמירה, ו-19% מהרשויות לא נקטו פעולות כלל בכדי לוודא את עמידת הגורם החיצוני בהוראות ההסכם והתקנות.

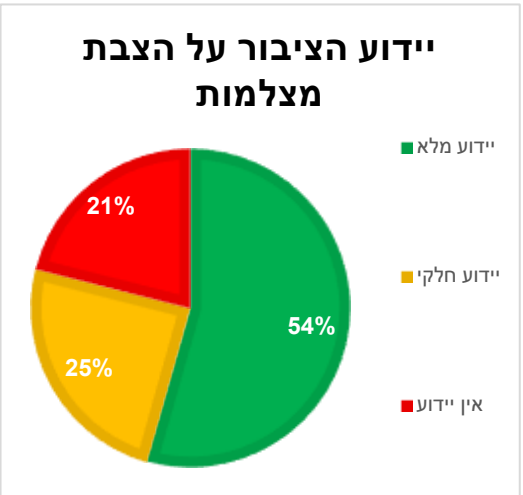


4.2.2. הצבה ושימוש במצלמות מעקב במרחב הציבורי

- ברשויות גדולות וקטנות, במאגרי מידע של מצלמות מעקב במרחב הציבורי, נמצא כי חלקן לא מבצעות שימוע ציבורי פומבי לצורך קבלת עמדת הציבור בדבר הצבת המצלמות ואף אינן מתייעצות עם בעלי עניין הנוגעים בדבר; לא קובעות רשימה מוגבלת של מורשי גישה לחומר המצולם; הצילומים נשמרים גם לאחר שאינם נחוצים עוד; אין ברשותן נהלים כתובים לשימוש במצלמות מעקב; ובחלק מן הרשויות הגדולות - לא הוצבו שלטים בסמוך למקום שבו מותקנת המצלמה.



- ממצאי הפיקוח עולה כי רק כמחצית (54%) מהרשויות המקומיות המבצעות שימוש במצלמות מעקב במרחב הציבורי מציבות שלטי יידוע בסמוך למצלמות באופן קריא וברור בנוסף למיפוי מלא של פריסת המצלמות באתר העירייה, בעוד שברבע מהרשויות (25%) בוצע יידוע של הציבור ע"י הצבת שלטי יידוע, אך הם אינם קריאים וברורים או שלא פורסמה רשימה מרוכזת של מיקומי המצלמות באתר האינטרנט של הרשות המקומית. ב-21% הנותרים לא הוצגו שלטים בסמוך למקום שבו מותקנת המצלמה.

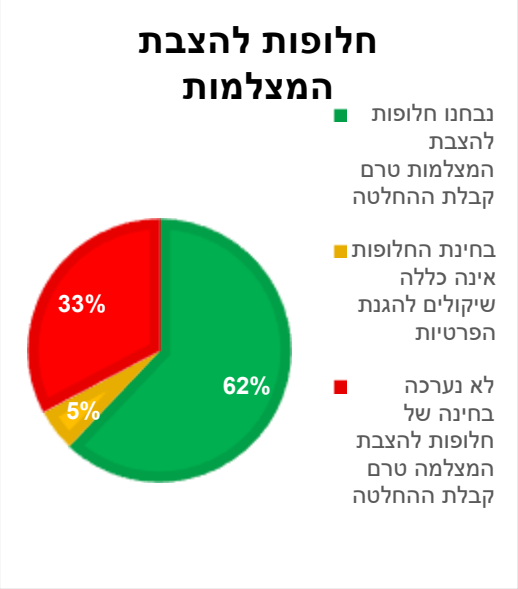


- עוד עולה מהליך פיקוח הרוחב, כי 92% מהרשויות המקומיות שנבדקו מבצעות שימוש במצלמות, כאשר מתוך הרשויות המקומיות המבצעות שימוש במצלמות

מעקב במרחב הציבורי, 80% מהן הגדירו מטרה להצבת המצלמות באופן חד, ספציפי ומפורש ובתחום סמכותה של הרשות המקומית. ביתר הרשויות הוגדרה מטרה אשר אינה קשורה לבעיה שפתרונה מצריך הצבת מצלמות, או שאינה בתחום סמכותה של הרשות המקומית (10%), או שכלל לא הוגדרה מטרה להצבת המצלמות (10%).

ב-64% מהרשויות בוצע שימוע ציבורי פומבי לצורך קבלת עמדת הציבור בדבר הצבת המצלמות, וב-36% מהן הציבור מודע לתכנון הצבת המצלמות אך עמדת הציבור לא נכללה בתסקיר.

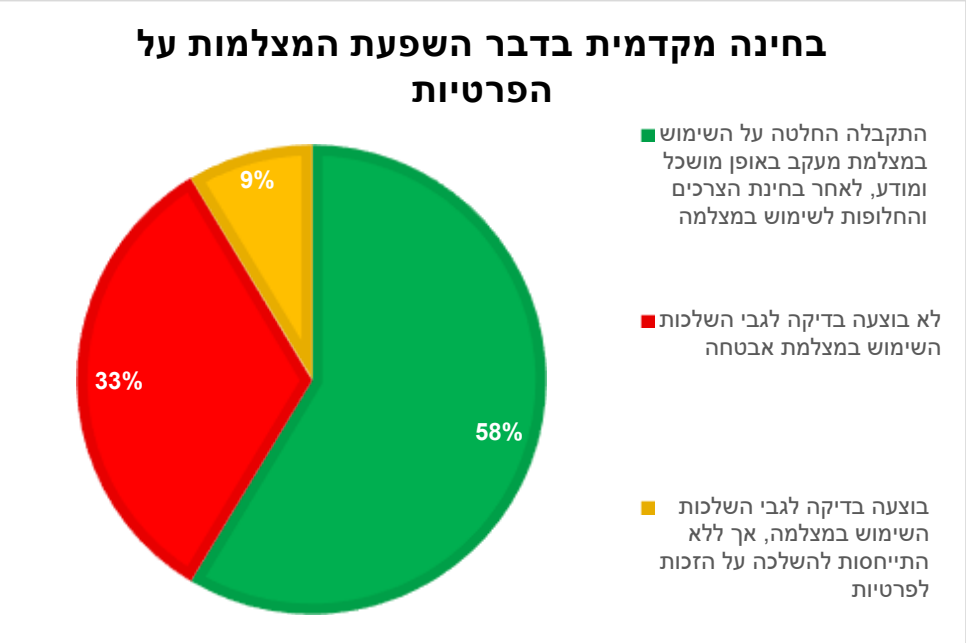
עוד עולה כי בעוד ש-62% מהרשויות מקפידות על בחינת חלופות להצבת המצלמות בטרם קבלת ההחלטה, בשליש מהרשויות (33%), כלל לא נערכה בחינה של חלופות להצבת המצלמה טרם קבלת ההחלטה, או שבחינת החלופות לא כללה שיקולים להגנת הפרטיות (5%).



בעניין השלכת מצלמות המעקב על פרטיות התושבים, ב-58% מהרשויות התקבלה החלטה על השימוש במצלמת מעקב באופן מושכל ומודע, לאחר בחינת הצרכים והחלופות לשימוש במצלמה, בעוד שבשאר הרשויות (33%) כלל לא בוצעה בדיקה לגבי השלכות השימוש במצלמות או שהבדיקה לא כללה התייחסות לזכות לפרטיות (9%).

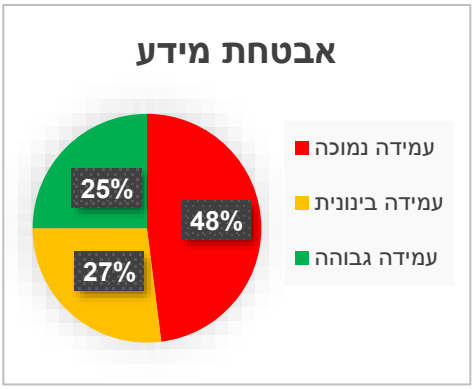
בעניין זה, נמצא באופן חיובי כי 84% מהרשויות אשר מבצעות שימוש במצלמות דיווחו כי כמות המצלמות אינה עולה על המינימום הנדרש, וכן נבדקו המיקום והזווית של המצלמות, כאשר ביתר הרשויות כמות המצלמות היא מעל המינימום הנדרש או שלא נבדקו מיקום וזווית המצלמות כנדרש.

יש לציין כי מבין הרשויות המבצעות שימוש במצלמות, עלה כי רמת אבטחת המידע של הקלטות הצילומים היא ברמה בינונית, כך שרק ב-65% מהרשויות קיימת הגנה פיסית ולוגית ראויה, בעוד שב-30% מהרשויות קיימת אבטחה בסיסית בלבד כגון חדר נעול במפתח או אימות באמצעות סיסמא חלשה, וב-5% מהן כלל לא קיימת הגנה פיזית/לוגית על מערכת מצלמות המעקב.



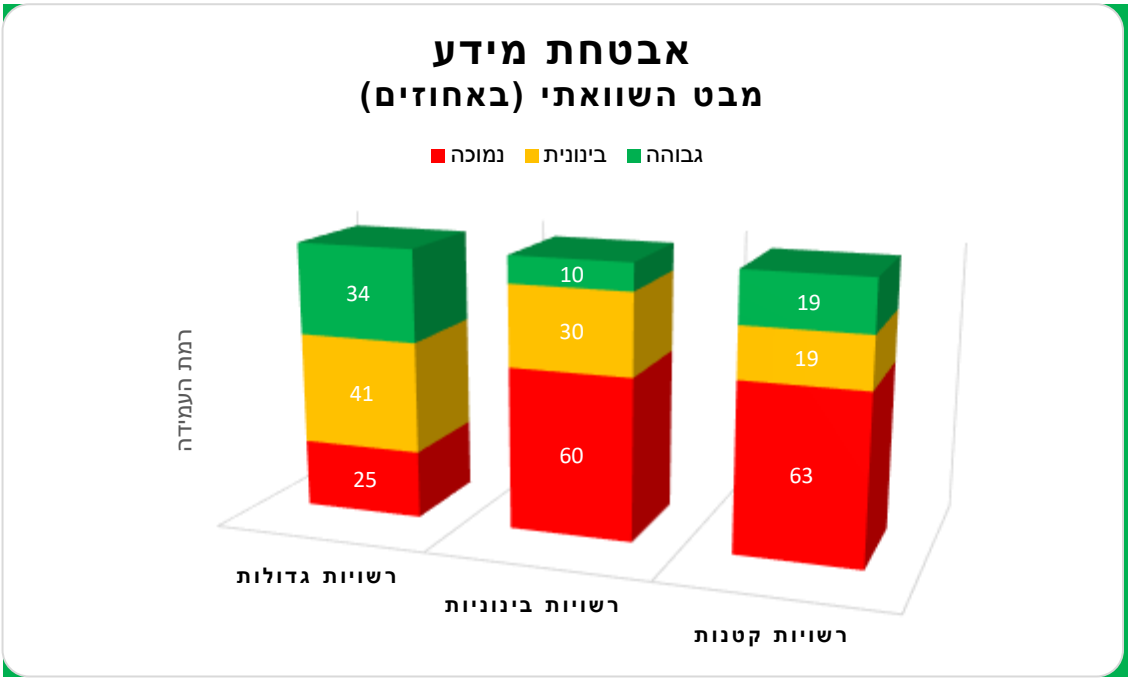
4.3. אבטחת המידע

במסגרת בחינת קריטריון זה, נמצא כי רק 25% מהרשויות המקומיות שנבדקו עמדו בהוראות החוק והתקנות בנושא אבטחת מידע ברמת עמידה גבוהה. ב-27% מהרשויות המקומיות שנבדקו נמצאה רמת עמידה בינונית, **וכמעט מחצית הרשויות שנבדקו (48%) נמצאו ברמת עמידה הנמוכה** בכל הנוגע ליישום הוראות החוק והתקנות בנושא זה.



במבט השוואתי, ניתן לראות יחס ישיר בין גודל הרשות לבין רמת העמידה שלה בהוראות החוק והתקנות בקריטריון אבטחת המידע. בקרב הרשויות המקומיות הגדולות, כרבע

מהרשויות עמדו ברמה נמוכה בדרישות אבטחת המידע הנדרשות בדין, **בעוד שבקרב הרשויות הבינוניות 60% עמדו ברמה נמוכה** ובאופן כללי רק 10% מהרשויות המקומיות עמדו ברמה גבוהה בדרישות אבטחת המידע, **ובקרב הרשויות הקטנות 63% עמדו ברמה נמוכה**.

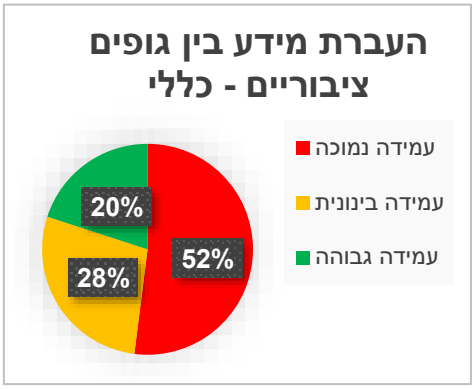


עיקר הליקויים בקריטריון זה נבעו מהסיבות שלהלן:

- בין הליקויים עלה כי בחלק גדול מהרשויות המקומיות כלל לא קיים נוהל אבטחת מידע, ובאלה שמחזיקות בנוהל, הוא כולל פחות מ- 50% מהסעיפים המפורטים בהוראות התקנות. גם בקרב הרשויות המקומיות הגדולות, בהן נמצא השיעור הגבוה ביותר של רשויות המחזיקות בנוהל אבטחת מידע, ב-63% מהן הנוהל אינו כולל את כל שנדרש לכלול בו על פי התקנות.
- חלק מהרשויות אינן מבצעות תיעוד של אירועים המעלים חשש לאירוע אבטחה כנדרש בתקנה 11 לתקנות.
- לא נערך סקר סיכונים או שלא בוצעו מבדקי חדירה למערכות המאגר בהתאם לדרישות בתקנה 5(ג), ובתקנה 5(ג) לתקנות.

- נמצאו ליקויים בנושא אבטחת אמצעים נתיקים, בין אם בהעדר הגבלות על שימוש באמצעים אלו, או בהעדר הצפנה נאותה.
- נמצאו רשויות מקומיות אשר לא נקטו באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את מאגרי המידע, או מאפשרים גישה אליהם.
- בחלק מהרשויות הקטנות והגדולות נמצא כי הכניסה למאגר על ידי עובד הארגון נעשית ללא שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה, בהתאם לדרישת תקנה 9(ב)(1), ובהיעדר מנגנון הרשאות גישה המבוסס על הצורך לדעת. כמו כן, בחלק ממערכות המאגרים ברשויות המקומיות לא קיימת מדיניות סיסמאות חזקה.
- לא קיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי לבין מערכות אחרות.
- נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בהעדר תהליכים נאותים לניהול הרשאות, ובין אם בהעדר יישום הפרדת תפקידים ויישום מתן הרשאה לפי עקרון הצורך לדעת בלבד (בעל ההרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות).

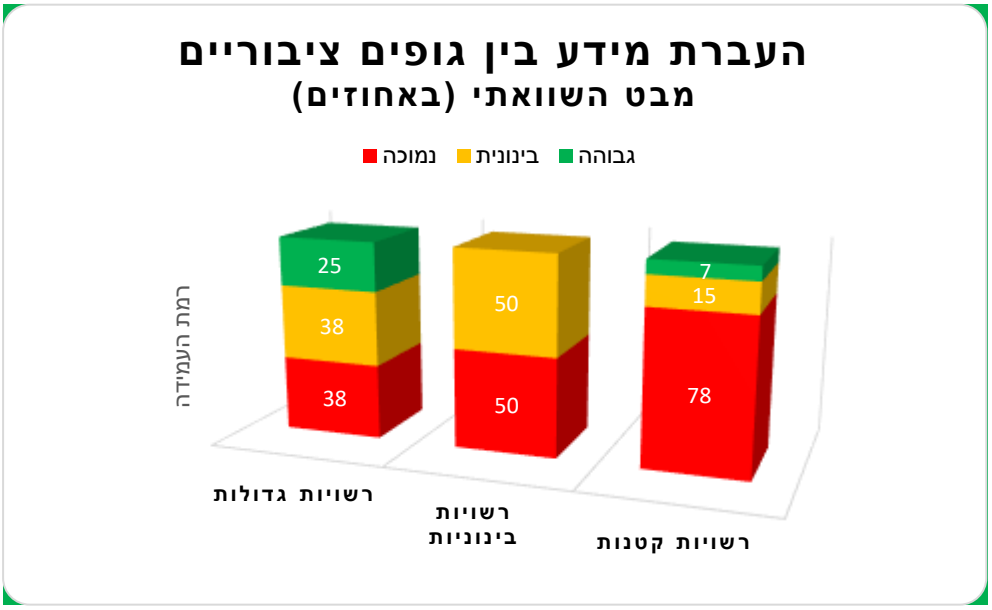
4.4. העברת מידע בין גופים ציבוריים



במסגרת בחינת קריטריון זה, נמצא כי רק 20% מכלל הרשויות שנבדקו עמדו ברמת עמידה גבוהה בהוראות החוק והתקנות בנושא העברת מידע בין גופים ציבוריים, בעוד שב-80% מהרשויות המקומיות נמצאה רמת עמידה בינונית או נמוכה, כאשר בפועל **למעלה ממחצית מכלל הרשויות שנבדקו (52%) נמצאו ברמת עמידה נמוכה** ביישום הוראות החוק והתקנות בנושא זה.

במבט השוואתי, גם בקריטריון זה ניתן לראות יחס ישיר מובהק בין גודל הרשות המקומית לבין רמת עמידה נאותה בהוראות החוק והתקנות באופן בו היא מעבירה מידע בין גופים ציבוריים. עם זאת, בקרב הרשויות המקומיות הגדולות, רק רבע מהרשויות ממלאות אחר

דרישות החוק והתקנות ברמה גבוהה בקריטריון זה, אחוז נמוך יחסית מזה המצופה מרשויות גדולות. **בקרב הרשויות המקומיות הבינוניות לא נמצאו רשויות הממלאות את דרישות החוק והתקנות ברמה גבוהה כלל, ומחצית מהן נמצאו ברמת עמידה נמוכה** בעוד המחצית השנייה ברמת עמידה בינונית בלבד. בקרב הרשויות המקומיות הקטנות נמצאה רמת עמידה נמוכה בהיקף הגדול ביותר, כאשר **78% מהרשויות הקטנות נמצאו ברמת עמידה נמוכה בקריטריון זה.**



עיקר הליקויים בקריטריון זה נבעו מהסיבות שלהלן:

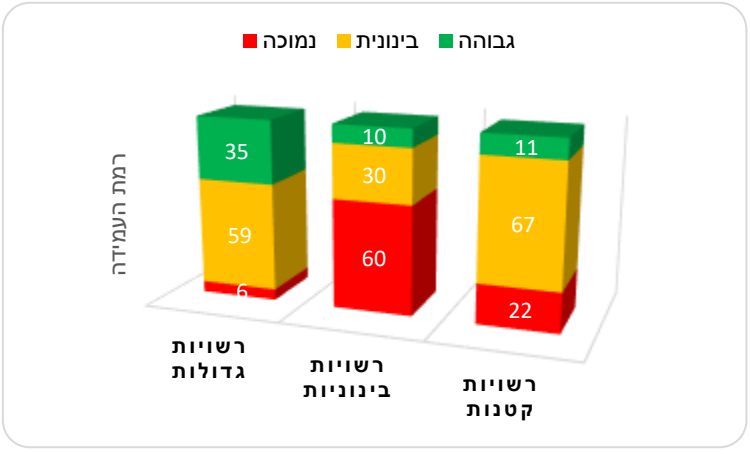
- עיקר הליקויים נבעו מאי הקמת וועדה להעברת מידע בין גופים ציבוריים בהתאם לנדרש בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986.
- נמצא כי הרשויות המקומיות אשר נמצאו ברמת עמידה נמוכה ובינונית כלל אינן מנהלות רישום בדבר העברות המידע (כנדרש בסעיפים 23ד(ב)-(ג) לחוק), וככל שמנוהל רישום כאמור, נמצא כי הוא אינו מנוהל באופן תקין או שמנוהל באופן חסר.
- נמצאו חוסרים במילוי נאות ושמירה של טופסי הבקשה להעברות מידע או של טופסי ההסכמה, ודיווח חסר או חלקי לרשות להגנת הפרטיות כנדרש בסעיף

23ד(ג) לחוק, לרבות אי רישום המידע שנמסר (כנדרש בסעיף 23ד(ב) לחוק) או רישום חלקי, ואי רישום קבלת מידע (כנדרש בסעיף 23ד(ג) לחוק) או רישום חלקי.

- כמו כן, נמצא כי חלק מהרשויות גם אינן מדווחות לרשות להגנת הפרטיות בדבר קבלת מידע המועבר דרך קבע, והמידע הנאגר במאגר המידע כנדרש בחוק ובתקנות.

5. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה, כי הגם שמרבית הרשויות במגזר רשויות מקומיות הינן בעלות היכרות עם דרישות החוק והתקנות, והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, **עדיין נמצאו ליקויים משמעותיים באופן יישום הוראות החוק והתקנות, כאשר עיקר הליקויים נמצאו בקרב הרשויות המקומיות הבינוניות והקטנות. בקרב הרשויות הבינוניות נמצא כי 90% מהן עמדו בהוראות החוק והתקנות ברמה בינונית או נמוכה, כאשר למעלה ממחציתן (60%) עמדו ברמה נמוכה. בקרב הרשויות הקטנות עמדו 89% בהוראות החוק והתקנות ברמה בינונית או נמוכה, וכשליש (30%) מהן עמדו ברמה נמוכה. גם בקרב הרשויות המקומיות הגדולות נמצאה רמת עמידה בינונית-נמוכה בקרב כשני שליש מהרשויות (66%), כאשר רק שליש מהן עמדו ברמה גבוהה (35%). נראה כי ברשויות בהן הוקצו משאבים וכוח אדם לנושא הגנת הפרטיות ואבטחת המידע (לרוב ברשויות גדולות, אך גם ברשויות קטנות אשר הקצו לכך משאבים), רמות העמידה היו באופן כללי גבוהות יותר, ומצופה מכלל הרשויות לנהוג בהתאם. נוכח הממצאים הנחיית הרשות היא כי על הרשויות המקומיות המשתייכות ליישם את הנקודות הבאות:**



5.1. בקרה ארגונית

נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשות הרשויות המקומיות, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותן, לרבות התאמה בין זהות מנהל המאגר על פי מסמכי הרשות המקומית, לבין הרשום אצל רשם מאגרי המידע.

על הרשויות המקומיות לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות עדכון פרטי מנהל המאגר בפנקס המאגרים ככל שמונה כזה, וכן מינוי ממונה אבטחת המידע, ולוודא שכתב המינוי כולל את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות אבטחת מידע.

בהתאם להוראות התקנות, יש לבצע הדרכות לגורמים האמורים אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. תיעוד החומרים שהועברו וכן תיעוד לביצוע ההדרכות – יישמר.

כמו כן, על הרשויות המקומיות לוודא כי קיימים נהלי אבטחת מידע בארגון. על הנהלים לכלול התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכד'. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות (תקנה 4).

כמו כן, על הרשויות המקומיות להכין תכנית עבודה לנושא אבטחת מידע והגנת הפרטיות, לרבות התייחסות לנושא גורם אחראי ולוחות זמנים לביצוע, שתעמוד בדרישות התקנות (תקנה 3 (3)). ככל שמדובר בגוף החייב במבדקי חדירות, עליו לוודא כי אכן נעשו כאלה וכי הם עומדים בדרישות התקנות (תקנה 16).

בנוסף, בהתאם לנדרש בתקנות (תקנה 7), על הרשויות המקומיות לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או כל גורם אחר שמקבל גישה למאגר או למערכת הכוללת מספר מאגרים.

5.2. ניהול מאגרי מידע

מכוח החובה המוטלת על פי החוק על רשויות מקומיות המנהלות מאגרי מידע על תושביהן, הכוללים אפיון של נושאי המידע לרבות מידע עליהם, כהגדרתו בחוק, נדרשות הרשויות לבצע מיפוי לכל מאגרי המידע הקיימים אצלן, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים, או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

על הרשויות המקומיות ליידע את התושב בדבר המקור החוקי לאיסוף המידע על אודותיו, ובכל מקום שאין סמכות חוקית כזו, לקבל את הסכמת התושב עבור שמירת פרטיו במאגריה. זאת, תוך מתן הודעה לתושב בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה עליו חובה חוקית למסור את המידע כאמור, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

על הרשויות המקומיות להקפיד לאפשר לתושבים לעיין במידע על אודותיהם, בהתאם להוראת סעיף 13 לחוק. לעניין זה יודגש, כי זכות העיון חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות, תכתובות צ'ט, שיחות המצולמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי על ידי הרשות המקומית או גוף אחר הנותן שירות לציבור. כמו כן, יש להקפיד ולאפשר לנושאי המידע לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע בהתאם לסעיף 14 לחוק, כאשר המידע אינו נכון, שלם, ברור או מעודכן.

5.2.1. עיבוד מידע אישי במיקור חוץ

בהתאם לתקנה 15 לתקנות אבטחת מידע על הרשויות המקומיות המסתייעות בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות. בנוסף, על הרשויות המקומיות בעלות המאגרים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל ההוראות המתחייבות על פי תקנה 15(א)(2) לתקנות אבטחת מידע, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.

כמו כן, על הרשויות המקומיות לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה 15.

5.2.2. מצלמות מעקב בשטח הציבורי

על הרשויות המקומיות לפעול על-פי דרישות החוק כפי שפורטו בהנחית רשם מאגרי מידע מס' 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן"[6] בכל הנוגע לאופן קבלת ההחלטה על הצבתן וההשלכות על זכויות הציבור, תוך בחינת חלופות אפשריות להצבת המצלמות, תכליתן ומידתיות השימוש בהן. כמו כן, יש לפעול בהתאם להנחיה לעניין מיקום התקנת המצלמות, כמות המצלמות, זמני הצילום, הרזולוציה ושימוש בפונקציות מיוחדות כגון זיהוי ביומטרי; יידוע הציבור בדבר הצבת המצלמות; אופן שמירת המידע המצולם ומחיקתו; זכות העיון של המצולם במידע; אופן אבטחת המידע הנאגר ממצלמות המעקב והגבלת השימוש במידע למטרה לשמה הוצבו המצלמות.

המלצות נוספות המתייחסות להיבטי "עיר חכמה", הכוללות שימוש שעושות רשויות מקומיות במצלמות מעקב וכן תחבורה במרחב העירוני ותיק תושב, ניתן למצוא במהדורה המחודשת של מדריך הגנת הפרטיות לעיר החכמה שפרסמה הרשות בינואר 2020.[7]

בכל הנוגע לשימוש במצלמות וידאו לצורך אכיפת עבירות חניה, על הרשויות לפעול בהתאם לחוזר מנכ"ל משרד הפנים מס' 4/2018 "נוהל שימוש במצלמות וידאו לצורך אכיפת עבירות חניה ברשויות המקומיות", אשר גובש בין היתר בסיוע הרשות להגנת הפרטיות.[8]

[6] הנחיית רשם מאגרי מידע מס' 2012/4 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן" - https://www.gov.il/BlobFolder/policy/surveillance_cameras_guidelines/he/The%20use%20of%20security%20cameras.pdf

[7] מדריך הגנת הפרטיות לעיר החכמה, ינואר 2020 - https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

[8] חוזר מנכ"ל 4/2018 – נוהל שימוש במצלמות וידאו לצורך אכיפת עבירות חניה ברשויות המקומיות - https://www.gov.il/BlobFolder/dynamiccollectorresultitem/notice-04-18/he/file_notice_notice-04-2018.pdf. ראו גם פסק הדין בבג"ץ 867/15 אור-הכהן נ' שר הפנים (16.5.18).

5.3. אבטחת מידע

נוכח הליקויים בנושא ניהול ההרשאות, על הרשויות המקומיות לוודא כי קיימים אצלן נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, כי הנהלים נבחנים מחדש מעת לעת כנדרש בתקנות, וכן לוודא בניית מנגנוני הרשאות במאגרי המידע של הארגון בהתאם לתקנות 8 ו-9 (א) לתקנות, אשר יבטיחו הפרדת סמכויות ויאפשרו גישה לנתוני המאגר אך ורק במידה הנדרשת לביצוע התפקיד של העובדים בעלי הגישה למידע.

בנוסף, על הרשויות המקומיות לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים או מאפשרים גישה אל מאגרי המידע. כמו כן, עליהן לוודא שבעת גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, כנדרש בתקנות (תקנה 9(ב)(2)).

במאגרים בעלי רמת אבטחה גבוהה יש לבצע מבדקי חדירה אחת ל-18 חודשים, בהתאם לתקנה 5(ד) לתקנות אבטחת מידע, וכן לוודא כי תיעוד של אירועי אבטחת מידע יישמר ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות.

כמו כן, נוכח הליקויים שנמצאו בנוגע לשימוש באמצעים נתיקים, מוצע כי הגורמים הרלוונטיים ברשויות המקומיות יקיימו דיון אודות הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שקיים צורך מינימאלי – עליהם להגביל השימוש למתכונת ההולמת את הפרמטרים הבאים: רמת אבטחת המידע שחלה על המאגר, רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד וקיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.

5.4. העברת מידע בין גופים ציבוריים

על הרשויות המקומיות לקבוע מדיניות ולהגדיר הנחיות ספציפיות לתחום העברת המידע בינם לבין גופים ציבוריים אחרים, בהתאם להוראות פרק ד' לחוק ולתקנות הייעודיות

בנושא[9]. בעניין זה ניתן להסתייע במדריך העברת מידע בין גופים ציבוריים שפרסמה הרשות,[10] ובטופס הדיווח המקוון המופיע במדריך ובאתר הרשות.[11]

עוד מוצע כי הרשויות המקומיות יבצעו פעולות פיקוח ובקרה תקופתיות (לכל הפחות עם סיומה של כל תקופת העברה), לווידוא יישום הוראות החוק והתקנות, ובכל הנוגע לשימוש במידע המתקבל אצלן מגופים ציבוריים אחרים.

6. סיכום

כאמור, מגזר הרשויות המקומיות מעלה סיכונים לא מעטים לפרטיות התושבים, אשר נובעים מניהול מידע רב, מזוהה ורגיש, ומניהול קשר ישיר עם ציבור התושבים באמצעות הרשויות המקומיות עצמן ובאמצעות גורמי מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות חוק הגנת הפרטיות, תקנות אבטחת מידע, ושקיפות מול התושב בנוגע לאיסוף ושימוש במידע על אודותיו.

ממצאי הליך פיקוח הרוחב שנערך כאמור בכ-70 רשויות מקומיות העלה ממצאים מדאיגים בקרב רשויות גדולות, בינוניות וקטנות, המצביעים על ליקויים בנוגע לעמידה בהוראות החוק בתחום ניהול מאגרי מידע, בקרה ארגונית ואבטחת המידע. נמצאו פערים בדבר עמידה בהוראות החוק בכל הנוגע למינויים של ממונה אבטחת מידע, ופערים ברמת האבטחה הקיימת ביחס לניהול הרשאות גישה למאגרי המידע. בנוסף, נמצא כי חלק מהרשויות המקומיות המשתייכות למגזר זה אינן מקפידות דיין ליידע את ציבור התושבים בדבר זכויותיו על פי חוק הגנת הפרטיות, הכוללות בין היתר את הזכות לעיין במידע.

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הרשויות המקומיות שנבדקו תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הרשויות המקומיות שבהתנהלותן נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית מסודרת לתיקונם.

[9] תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986.
[10] מדריך העברת מידע בין גופים ציבוריים - https://www.gov.il/BlobFolder/service/information_flow_between_public_bodies/he/info-bulletin.pdf
[11] https://www.gov.il/he/Departments/Guides/public_organizations_data_transfer2?chapterIndex=6

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלים ומחזיקים במאגרי מידע אישי באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות ברשויות המקומיות שהונחו לתקן ליקויים, וזאת לשם הגברת עמידתן בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על זכות הציבור לפרטיות.

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות להמשיך ולבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר הרשויות המקומיות, על ידי בחינת רשויות מקומיות נוספות, במועד שייקבע לאחר פרסום דוח זה.

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית			
לא מונה ממונה אבטחת מידע.	בהתאם לסעיף 17ב לחוק, מעצם היותך גוף ציבורי יש לפעול למינוי ממונה על אבטחת המידע .	סעיף 17ב לחוק	**מינוי ממונה אבטחת מידע**
לא קיים נוהל אבטחת מידע או שנוהל אבטחת מידע כולל פחות מ- 50% מהסעיפים המפורטים בתקנות	כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נוהל אבטחת מידע**
לא קיימת תכנית עבודה שנתית	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות המפרטת את הגורם האחראי ואבני דרך ברורות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה שנתית**
לא קיים הליך מיון של עובדים חדשים (הנגישים למאגר מידע)	הטמעת תהליך מיון של עובדים חדשים שבוחן היבטים הרלבנטיים לפרטיות ולאבטחת מידע.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(א), תקנה 23	**מיון עובדים**
עובדים חדשים לא עוברים הדרכה או שתדירות ההדרכות היא פחות מפעם בשנתיים או שההדרכות אינן מכסות את נושא אבטחת מידע והגנת הפרטיות בצורה מספקת-	יש לקבוע הדרכות לפחות פעם בשנתיים במאגרים שחלה עליהם רמת האבטחה הבינונית או הגבוהה בנושא אבטחת מידע והגנת הפרטיות בצורה מספקת וניהול תיעוד ומעקב אחר הדרכות אלו.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(ג)	**הדרכות לעובדים**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא בוצע סקר סיכונים או ביקורות בנושא אבטחת מידע והגנת הפרטיות בשלוש השנים האחרונות	השלמת התהליך בהקדם וביצוע ביקורת בנושא אבטחת מידע וכן סקר סיכונים. עריכת ביקורות בנושא אבטחת מידע והגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה. לחלופין במאגר ברמת אבטחה גבוהה - עריכת סקר סיכונים מידי 18 חודשים הכולל את דרישות הביקורת.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5, תקנה 16	**סקר סיכונים/ביקורת אבטחת מידע**
ניהול מאגרי מידע			
לא ניתנת הודעה בהתאם לדרישות סעיף 11 לחוק.	מתן הודעה לתושב בעת איסוף המידע. על נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11	**מתן הודעה לנושא המידע**
לא ניתן לנושא המידע לעיין במידע על אודותיו כנדרש בסעיף 13 לחוק, או שניתנת לו אפשרות לעיין באופן חלקי בלבד	יש לאפשר לנושא המידע לעיין במידע שעליו המוחזק במאגר המידע.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13	**עיון במידע**
לא מתאפשר לנושא המידע לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק בשיעור גבוה מהרשויות	יש לאפשר לתושב לתקן את המידע המוחזק בעניינו ברשות, אם נמצא כי המידע אינו נכון, שלם, ברור או מעודכן.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 14	**שינוי/תיקון המידע**
לא עוגנו הסכמי התקשרות עם ספקי מיקור חוץ המכילים את מלוא הפרטים הנדרשים בהתאם לתקנות.	יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות: 1. דיווח אודות אירועי אבטחת מידע. 2. מנגנוני אבטחת המידע הנדרשים. 3. שמירת המידע לאחר סיום תקופת	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
	ההתקשרות. 4. חובות גורם חיצוני בהעברת מידע לאחר.		
לא קיים הסכם מול ספק מיקור החוץ.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 והנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי בחברה, לרבות נקיטת אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**
לא ננקטות פעולות לוודא כי גורם חיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש.	ווידוא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15	**מיקור חוץ**
העברת מידע בין גופים ציבוריים			
לא הוקמה וועדה להעברת מידע בין גופים ציבוריים.	בהתאם לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986, יש להקים וועדה מקצועית לנושא העברת מידע בין גופים ציבוריים כנדרש בתקנות. המנהל הכללי או מזכיר הרשות המקומית או סגנו יהיה יושב ראש הוועדה. בוועדה ישמשו היועץ המשפטי או נציגו וממונה אבטחת המידע. מספר חברי הוועדה לא יפחת משלושה.	תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986	**וועדות**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
מונתה וועדה אך טרם התכנסה.	יש לוודא כי הוועדה להעברת מידע בין גופים ציבוריים התכנסה לצורך דיון בניהול מידע ואבטחתו.	תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986	**וועדות**
לא מבוצע רישום למידע שנמסר.	גוף ציבורי המוסר דרך קבע מידע בהתאם לסעיף 23ג יפרט עובדה זו, כמו כן, יקיים רישום של המידע שנמסר.	חוק הגנת הפרטיות, תשמ"א-1981, סעיף 23ד	**רישום המידע שנמסר**
אבטחת מידע			
אין אמצעי אבטחה פיזיים למניעת גישה לשרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע.	יש להבטיח כי המערכות יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות ושל כל הכנסה והוצאה אל מערכות המאגר ומהן.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017,תקנה 6	**אבטחה פיזית**
לא קיים תיעוד של אירועי אבטחה.	יש לתעד כל אירוע המעלה חשש לאירוע אבטחה. בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחה מידע. במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.	תיעוד של אירועי אבטחה תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 11	**תיעוד אירועי אבטחה**
קיימת אפשרות לחבר התקנים ניידים ואין הצפנה.	הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 12	**הצפנת התקנים ניידים**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
	כאמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.		
לא קיים מנגנון הרשאות או שמנגנון ההרשאות מאפשר לבעלי תפקידים לגשת לנתונים במאגר למרות שאין בכך צורך	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 8, תקנה 9	**מנגנון הרשאות**
לא ננקטים אמצעים סבירים לצורך ווידוא כי הגישה למאגרים נעשית בידי בעלי ההרשאה בלבד למאגר המידע/מערכת מידע.	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 8, תקנה 9 (א)	**מנגנון הרשאות**
לא קיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי ליתר המאגרים	יש לקיים הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	ניהול מאובטח ומעודכן של מערכות המאגר תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב)	**הפרדת מאגרים עם מידע שונה**
בכניסה למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	במאגרים שחלה עליהם רמת אבטחתה בינונית ומעלה, אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. כגון תעודה המכילה חתימה אלקטרונית מאובטחת, TOKEN וכדומה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב-1)	**שימוש באמצעי פיזי מרחוק**
לא קיימת מדיניות סיסמאות חזקה.	במאגרים בעלי רמת אבטחה בינונית ומעלה, קביעה בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה, הכוללת בין היתר:	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב)	**מדיניות סיסמאות**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
	סיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכדומה.		
לא נערך סקר סיכונים בשנה וחצי האחרונות	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים מדי שנה וחצי, ותיקון הליקויים שהתגלו במסגרת הסקר.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ג)	**סקר סיכונים**
לא נערכו מבדקי חדירה בשלוש השנים האחרונות על ידי גורם מקצועי.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה אחת לשנה וחצי, בחינת הצורך בעדכון נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.	מבדקי חדירות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ד)	**מבדקי חדירה**