ביקורת בנושא

ניהול מאגרי מידע בעירייית קריית ביאליק לשנים 2015-2017

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

עיריית קריית ביאליק **Municipality of Qiryat Bialik**
היחידה לביקורת פנים ופניות הציבור
רחוב שד' ירושלים 16, קריית ביאליק 27100
טלפון: 04-8780808 פקס: 04-8781705

תאריך: 24/10/2017
מספרנו: 41397

ביקורת בנושא ניהול מאגרי מידע

תקציר מנהלים

להלן עיקרי ממצאים, מסקנות והמלצות מדו"ח ביקורת שנערך בעיריית קריית ביאליק, בנושא: ניהול מאגרי מידע.

***לשם קבלות החלטות רצוי לעיין בדו"ח המלא**

1. רקע

1.1. הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל. עניינה של הזכות לפרטיות הוא בשמירה על האוטונומיה של האדם, בשמירה על צנעת חייו ועניינו האישיים ואף בהגנה על האדם מפני שימוש לרעה במידע על אודותיו. מאגרי מידע מסכנים בעצם קיומם את הפרטיות, ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

1.2. איסוף המידע כיום פשוט מבעבר, וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים, בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות".

1.3. בעירייה ישנם 11 מאגרי מידע.

1.4. יחידת מערכות המידע בעירייה אמונה על מתן שירותי מחשב לעובדי העירייה, ניהול המשתמשים, אבטחת המידע ותפעול שוטף של מערכות המחשב בעירייה.

1.5. במהלך החודשים מרץ ועד אוקטובר 2017 בוצעה ביקורת בעיריית קריית ביאליק.

1.6. הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר העירייה לשנת 2017.

2. פרק 2 - מנהל אבטחת מידע

נמצא כי העירייה מינתה עובד ייעודי העוסק בתחום אבטחת המידע, אולם לא מונה כמפקח האחראי על תחום מאגרי המידע.

3. פרק 3 - מבנה ארגוני

נמצא כי בניגוד להנחיות אגף משאבי אנוש במשרד הפנים הקובעות כי המנמ"ר יהיה כפוף מנהלתית למנכ"ל העירייה, המנמ"ר כפוף לגזבר העירייה.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

4. <u>פרק 4 - ועדת היגוי לאבטחת מידע</u>

בעירייה לא הוקמה וועדת היגוי לאבטחת מידע ולפיכך גם לא נכתב נוהל לפעילות וועדת ההיגוי לאבטחת מידע.

5. <u>פרק 5 - מדיניות אבטחת מידע ותכנית עבודה</u>

5.1. בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות ונוהל אשר מפרט כיצד על המחלקה ועל המשתמשים בעירייה להתנהל בתחום המיחשוב בכלל ובתחום אבטחת המידע בפרט. על הנוהל לכלול פרטים נדרשים , כגון: הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר, הרשאות גישה למאגר המידע ולמערכות המאגר, תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך, הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר, הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר, אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר; אופן התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע; הוראות לעניין ניהול של התקנים ניידים ושימוש בהם,

5.2. הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת וכן לא בוצע מיפוי וסקר סיכונים.

6. <u>פרק 6 - טיפול באירועי אבטחת מידע</u>

6.1. לא קיים נוהל עירייה פנימי אשר מנחה מהו הטיפול הנדרש באירועי אבטחת מידע.

6.2. לא קיים תיעוד כלשהו באשר לאירועי אבטחת מידע שהתרחשו (אם התרחשו) במהלך השנים בעירייה.

6.3. לא קיימים בעירייה כלי ניטור על פעילות המשתמשים. לדוגמא, משתמשים אשר מתחברים שלא בשעות העבודה, משתמשים שטועים בסיסמא שלהם ולפיכך מתנתקים, משתמשים שמנקודת התקשורת שלהם מתחבר מחשב שאינו מחשב של העירייה וכיו"ב.

7. <u>פרק 7 - ניהול מאגרי המידע</u>

מבדיקת הביקורת עולה כי כל מאגרי המידע הקיימים בעירייה מנוהלים בעירייה ללא שנרשמו בפנקס אצל רשם מאגרי המידע, במשרד המשפטים.

8. <u>פרק 8 - הגשת בקשה לרישום מאגר מידע לרשם</u>

העירייה לא רשמה את מאגרי המידע ברשם מאגרי המידע ולפיכך , גם לא הגישה בקשה לרישום המאגרים בהתאם להוראות סעיף 9 לחוק הגנת הפרטיות.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

9. <u>פרק 9 - בעל הרשאה</u>

9.1. נמצא כי ב 7 – מתוך 10 החברות החיצוניות שעובדות עם העירייה ושקיבלו הרשאה להחזיק במידע לא חתמו על הסכם סודיות.

9.2. ב- 5 מתוך 10 החברות שנבדקו , לא נחתם כלל הסכם התקשרות בין החברה לעירייה.

9.3. העירייה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך הגדילה את הסיכוי לפגיעה במאגרי המידע העירוניים.

10. <u>פרק 10 - מיקור חוץ</u>

ב- 7 מתוך 10 החברות שנבדקו נמצא כי החברות לא חתמו על טופס התחייבות לשמירת סודיות וכן בטרם ביצוע ההתקשרות לא בוצע סקר סיכונים לצורך אבטחת המידע.

11. <u>פרק 11 – ההיבט האזרחי, הפלילי והעונשי</u>

11.1. אי רישום של מאגר מידע החייב ברישום מבלי שנרשם, מהווה עבירה פלילית שדינה מאסר שנה, לפי סעיף 31א(א)(1) לחוק הגנת הפרטיות.

11.2. בנוסף, ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה בגינה רשאי רשם מאגרי מידע להטיל קנס מינהלי.

12. <u>פרק 12 – שקיפות</u>

בעירייה ישנם 11 מאגרי מידע, אולם בדוח לתושב נרשם כי ישנם 4 מאגרי מידע ובאתר האינטרנט העירוני נרשם כי ישנם 5 מאגרי מידע ולכן הביקורת מעירה כי יש לפרסם באתר העירייה ובדוח לתושב את כלל מאגרי המידע הקיימים.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

להלן הדו"ח המלא

דו"ח ביקורת בנושא ניהול מאגרי מידע

1. מבוא

1.1. הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל. עניינה של הזכות לפרטיות הוא בשמירה על האוטונומיה של האדם, בשמירה על צנעת חייו ועניניו האישיים ואף בהגנה על האדם מפני שימוש לרעה במידע על אודותיו. עם חקיקת חוק יסוד: כבוד האדם וחירותו אף הוקנה לה מעמד חוקתי על חוקי. סעיף 11 לחוק היסוד קובע כי "כל רשות מרשויות השלטון חייבת לכבד את הזכויות שלפי חוק יסוד זה". כמו כן, הזכויות החוקתיות לכבוד ולפרטיות מטילות על המדינה חובה להגשימן באמצעים העומדים לרשותה[1].

1.2. מידע פרטי הוא בעל ערך רב, לרבות ערך כלכלי, ולכן לחברות מסחריות ולגופים אחרים אינטרס ברור באיסופו ובשמירתו במאגרי מידע. בנוסף, בידי רשויות המדינה מידע רב על בני אדם, הנוגע לכל היבטי חייהם, וקיים חשש שייעשה בו שימוש שלא למטרה שלשמה הוסמכו הרשויות לאספו. מאגרי מידע מסכנים בעצם קיומם את הפרטיות[2], ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

1.3. צורך זה מתעצם בשל ההתפתחות הטכנולוגית מרחיקת הלכת של העשורים האחרונים, שהביאה עמה שינויים באופן שבו מידע נאסף ומעובד ובשימושים הנעשים בו. איסוף המידע כיום פשוט מבעבר, וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים, כגון גלישה באינטרנט או תשלום בכרטיס אשראי, תוך הצלבת נתונים אלה עם נתונים אחרים וביצוע חיתוכים במידע שנאסף. כתוצאה מכך, נוצרו איומים חדשים על הזכות לפרטיות במידע. בהתייחס לכך ציין בית המשפט העליון[3] כי "אמצעי המחשוב המודרניים והטכנולוגיה המתקדמת בתחום התקשורת מביאים עמם ברכה רבה בצד סכנות גוברות לפגיעה בזכותו של האדם לפרטיות".

1.4. בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות"[4]. בשל הפגיעה הפוטנציאלית הגלומה במאגרי מידע יוחד בחוק פרק לנושא זה, ונקבעה בו חובה לרשום מאגרי מידע[5]. לפני ניהולם והחזקתם, בפנקס המנוהל על ידי רשם מאגרי המידע. במרוצת השנים הוטלו אגרה עבור רישום מאגרי מידע ואגרה תקופתית על מאגרי מידע רשומים. מטרת הרישום היא לאפשר בקרה ופיקוח על המאגרים, להביא להגנה על פרטיות המידע ולאפשר לציבור לדעת על קיומו של מידע על אודותיו במאגרי המידע. לצד חובת הרישום, מטיל החוק חובות מהותיות על בעל מאגר מידע והמחזיק בו, בהן אחריות לאבטחת המידע האגור במאגר, שמירת סודיות המידע והימנעות משימוש בו שלא למטרה שלשמה נמסר.

1.5. בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום. במהלך השנים השתנתה מציאות זו לחלוטין, ובשנים האחרונות רווחת

---

[1] בג"ץ 2557/05 **מטה הרוב נ' ממשלת ישראל**, פ"ד סב(1) 200, פסקה 4 לפסק דינו של הנשיא ברק (2006); ע"ע (ארצי) 90/08 **איסקוב נ' מדינת ישראל - הממונה על חוק עבודת נשים**, פסקה 11 לפסק הדין (פורסם במאגר מידע, 8.2.11).

[2] עת"מ (ת"א) 24867-02-11 **איי.די.איי חברה לביטוח בע"מ נ' רשם מאגרי המידע, הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים**, פיסקה 6 (פורסם במאגר מידע, 1.8.12).

[3] בג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פ"ד נח(4) 842, 864.

[4] ה"ח 1453 התש"ם, 206.

[5] סעיף 8(ג) לחוק קובע שבעל מאגר מידע חייב ברישומו בפנקס אם מתקיימת בו אחת מהנסיבות המנויות בסעיף, בהן שמספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000 ; המאגר מכיל מידע רגיש כהגדרתו בחוק ; המאגר משמש לשירותי דיוור ישיר.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

ההערכה כי ישנם בישראל מיליוני מאגרי מידע החייבים, על פי הוראות החוק, ברישום. כמעט לכל בית עסק לפחות מאגר מידע אחד החייב ברישום, ואף רבים מהטלפונים החכמים שבידי אנשים פרטיים מכילים מאגרי מידע החייבים, לכאורה, ברישום .

2. <u>רקע ייחודי לקריית ביאליק:</u>

2.1. פעולתם של גופים ציבוריים מושתתת על מערכות מידע הכוללות נתונים רבים על התושבים מעמד אישי, מצב בריאות, מצב כלכלי, הכשרה מקצועית, דעות ואמונות שחשיפתם עלולה לפגוע בפרטיותם של התושבים. ככל שהגופים עושים שימוש נרחב יותר במאגרי המידע כך גוברת הסכנה שהמידע ייחשף ברבים ויפגע בפרטיותם של התושבים, ולכן מוטלת על בעלי המאגרים החובה להגן על המידע.

2.2. בעירייה פועלות מערכות מידע ממוחשבות רבות החיוניות להבטחת תקינות פעילותה השוטפת בתחומים האלה: כספים (גבייה, שכר, תשלומים לספקים ועוד); תכנון ובנייה; חינוך (שירות פסיכולוגי חינוכי, גני ילדים, קייטנות ועוד); רווחה; כוח אדם; רישוי עסקים; תחבורה וחניה; תברואה ועוד. מאגרים אלה הם הבסיס לעבודתם של הרשויות.

2.3. בעירייה ישנם 11 מאגרי מידע, בהתאם לפירוט הבא:

<u>רשימת מאגרי מידע</u>

<u>מס"ד</u>	<u>מחלקה</u>	<u>מאגרים</u>	<u>חברה מחזיקה</u>
1	גביה	ארנונה, שילוט, מרשם אוכלוסין (מימד)	מטרופולינט, מגע"ר, זיצר
2	הנהלת חשבונות+ רכש	מאגר ספקים,	מטרופולינט, זיצר
3	משאבי אנוש ושכר	משכורות עובדים, פרטי עובדים וגמלאים	אוטומציה, סינאל
4	חינוך וגני ילדים	רישום תלמידים וילדים, מערכת ניהול כספים	מטרופולינט
5	פיקוח עירוני	דוחות חניה	מטרופולינט
6	רישוי עסקים	מעקב אחר רישיונות עסק לעסקים בעיר	רמה מערכות
7	וטרינר עירוני	ניהול פרטי מחזיקי בעלי הכלבים המחוסנים ב- 3 רשויות	סורין הרשקו
8	רווחה	מטופלי רווחה	מטרופולינט
9	חברת קדישא	מאגר נפטרים	כרמל
10	מרכז הספורט "אפק"	ניהול רשימת מנויים	Expo
11	ספרייה עירונית	מנויי ספרייה	אגרון פלוס

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

3. <u>חוקים, הוראות ונהלים</u>

3.1. פקודת העיריות, נוסח חדש, תשכ"ד 1964.

3.2. חוק יסוד כבוד האדם וחירותו על פיו "כל אדם זכאי לפרטיות ולצנעת חיו".

3.3. חוק הגנת הפרטיות, תשמ"א- 1981 (להלן: "חוק הגנת הפרטיות")

3.4. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבורים), תשמ"ו- 1986

3.5. חוק המחשבים, התשנ"ה- 1995.

3.6. חוק העונשין, תשל"ז-1977 הקובע את העונשים החלים על עובדי ציבור שמוסרים מידע שלא כחוק.

3.7. חוק להסדרת ביטחון בגופים ציבוריים, התשנ"ח- 1889, הקובע את דרכי הפעולה והניהול של הביטחון ובכלל זה אבטחת מידע ממוחשב ומידע פיזי רשומות בגופים ציבוריים.

3.8. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017.

3.9. נהלי מסגרת לאבטחת מידע משרד ראש הממשלה של אגף בכיר לביקורת המדינה והביקורת הפנימית המועצה המייעצת לביקורת ואבטחת מידע, הרשות הלאומית להגנת הסייבר, ספטמבר 2005 .

4. <u>מטרות הביקורת</u>

4.1. איתור חריגות מחוקים, הוראות ונוהלי עבודה.

4.2. איתור חריגות מסמכויות.

4.3. איתור סיכונים עסקיים ותפעוליים.

4.4. איתור ליקויים מערכתיים (כגון: חסר או ליקוי בנהלים, ליקויי תוכנה).

4.5. איתור מקרים בהם קיים חשד לפגיעה בטוהר מידות מצד עובדי העירייה.

4.6. איתור מקרים בהם קיימת פגיעה בחיסכון, בשמירה על הרכוש וביעילות העבודה.

4.7. הביקורת בחנה את ההיבטים השונים הקשורים לנושא ניהול מאגרי מידע:

4.8. כמו כן, הביקורת בדקה האם פעילות העירייה בתחום מאגרי מידע מתבצעת תוך שמירה על חוקיות, סדירות, עקרון השוויון, חסכון, יעילות שקיפות ומניעת פגיעה בטוהר המידות.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

5. **<u>היקף הביקורת ואופן הבדיקה</u>**

5.1. במהלך החודשים מרץ ועד אוקטובר 2017 בוצעה ביקורת בעיריית קריית ביאליק.

5.2. הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר העירייה לשנת 2017. הנושא נכלל בתכנית העבודה השנתית, בשל דרישת ראש העיר ובהתאם לסמכותו בחוק.

5.3. הביקורת הסתמכה על הוראות החוק כפי שמופיעות בסעיף 3 בדו"ח זה.

5.4. הביקורת בוצעה ע"י גב' שלי דרעי וגב' מאיה ליבונטי-מיארה סטודנטיות לביקורת באוניברסיטת חיפה וע"י מר אייל לוי, המבקר הפנימי.

5.5. <u>לצורך ביצוע המטלה, הביקורת קיבלה נתונים</u>:

- מאגף הכספים , גזבר העירייה ומצוות האגף.
- מהמחלקה המשפטית.
- ממנהל מערכות המידע של הרשות.
- חוזים והתקשרויות עם ספקים.

5.6. הביקורת בחנה את ההתנהלות העירייה ביחס לניהול מאגרי מידע בעיריית קריית ביאליק בין השנים 2015-2017 וכללה את ההיבטים הבאים:

6. **<u>עזרים לביצוע הביקורת</u>**

6.1. נתונים מאגף הגזברות.

6.2. נתונים מאת המחלקה המשפטית.

6.3. נהלי עבודה עירוניים.

6.4. חוזי התקשרות עם ספקי שרות.

6.5. אתר האינטרנט העירוני.

6.6. דוח ביקורת בתחום "אבטחת מידע" שנעשה על ידי מבקר עיריית עכו.

6.7. דוח מבקר המדינה מספר 64ג', משנת 2014 בנושא רישום מאגרי מידע בישראל.

7. **<u>הגדרות</u>**

7.1. **"מאגר מידע"** - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט –

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

7.2. **"מידע"** - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

7.3. **"מנהל מאגר"** - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

להלן ממצאי הביקורת

1. כללי

יחידת מערכות המידע בעירייה אמונה על מתן שירותי מחשב לעובדי העירייה, ניהול המשתמשים, אבטחת המידע ותפעול שוטף של מערכות המחשב בעירייה.
היחידה מטפלת בכ- 2,000 מחשבים / שרתים. לצורך ביצוע חלק ממשימותיהם, על היחידה לעבור פיזית בין אתרים שונים בהם נמצאים מחשבי ושרתי העירייה.

2. מנהל אבטחת מידע

2.1. בסעיף 17 ב. (א) לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

"הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):"

2.2. הוראה זו חלה גם על רשויות מקומיות, שכן הן נכללות בהגדרה של רשויות ציבוריות, על פי הגדרות החוק.

משרד הפנים קבע הגדרת תפקיד לתפקיד מנהל אבטחת מידע (Chief Security Office),

במסגרתה נקבעו תחומי האחריות של הממונה, כפיפותו למנהל מערכות מידע ראשי

(מנמ"ר) וכן 4 דרישות סף לקבלה לתפקיד:

- בעל תעודת טכנאי או הנדסאי
- ידיעת השפות עברית ואנגלית ברמה גבוהה
- נסיון מקצועי - ברשות מקומית ברמה ב' וג' ניסיון מקצועי של שנה לפחות כמנהל או כסגן -מנהל מערכות מידע, או מנהל אבטחת מידע בחברה בעלת 25 עובדים ומעלה.
- היעדר עבר פלילי - היעדר הרשעה בעבירה שבנסיבות העניין יש עמה קלון.

2.3. **נמצא כי העירייה מינתה עובד ייעודי העוסק בתחום אבטחת המידע, אולם לא מונה כמפקח האחראי על תחום מאגרי המידע.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

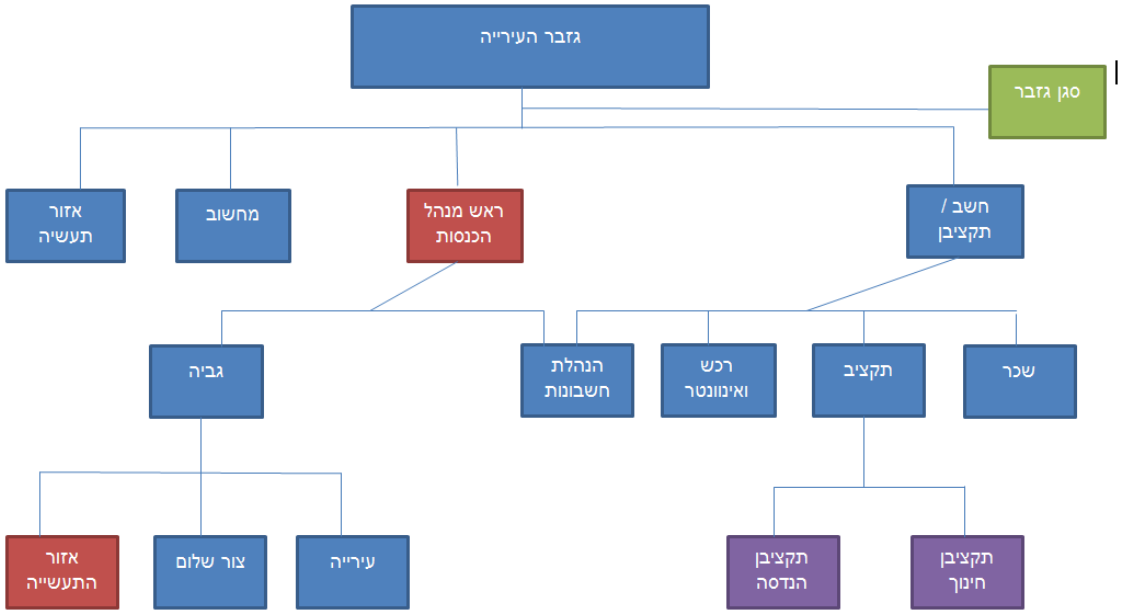
3. מבנה ארגוני

3.1. האגף לכח אדם ושכר ברשויות מקומיות במשרד הפנים קובע כי יש למנות מנהל מערכות מידע ראשי (מנמ"ר), אשר יתכנן וינהל את מערכות המידע הניהוליות של הרשות המקומית. בין היתר, נקבע כי ברשות מקומית ברמה א' המנמ"ר יהיה כפוף למנכ"ל או סמנכ"ל הרשות, וכי ברשות מקומית ברמה ב' או ג', המנמ"ר יהיה כפוף למנכ"ל או מזכ"ל הרשות.

3.2. **נמצא כי בניגוד להנחיות אגף משאבי אנוש במשרד הפנים הקובעות כי המנמ"ר יהיה כפוף מנהלתית למנכ"ל העירייה, המנמ"ר כפוף לגזבר העירייה.**

להלן המבנה הארגוני של אגף הכספים:

מבנה אגף כספים



תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

4. <u>ועדת היגוי לאבטחת מידע</u>

4.1. נוהל מס׳ 5 לנהלי המסגרת בנושא ״ועדות היגוי למחשוב ואבטחת מידע״ קובע כי ועדת ההיגוי תתכנס לפחות פעמיים בשנה ותורכב מנושאי המשרה הבאים:

- סמנכ״ל בכיר
- מנהל אגף מחשוב
- חשב/ גזבר
- המבקר הפנימי
- נציג היועץ המשפטי
- קצין הביטחון
- הממונה על אבטחת מידע

<u>הנוהל קובע כי הועדה תעסוק, בין היתר, בנושאים הבאים:</u>

- קביעת מדיניות המחשוב ואבטחת מידע.
- אישור תוכנית עבודה שנתית בתחום אבטחת המידע, לרבות תקציבים, לוחות זמנים ותחומי אחריות.
- קבלת דיווחים ומעקב ביצוע בנושאי אבטחת מידע.
- סיווג המידע (רגיש/ סודי/ אישי/ פומבי).

4.2. **לא קיים בעירייה נוהל העוסק בפעילות וועדת היגוי לאבטחת מידע.**

4.3. **לא קיימת בעירייה וועדת היגוי לאבטחת מידע, וממילא לא מתכנסת וועדה, כנדרש בנוהל מסגרת מס׳ 5.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ״ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** ״ לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור.״

סעיף 334א. ״ המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה.״

5. <u>מדיניות אבטחת מידע ותכנית עבודה</u>

5.1. <u>מסמך מדיניות</u>

נוהל מספר 1 לנוהלי המסגרת בנושא "קביעת מדיניות אבטחת 'מידע רגיש' ומערכי מידע בממשלה ומוסדותיה" קובע כי יש להכין מסמך "מדיניות אבטחת המידע הרגיש ומערכי המידע" ולהטמיעו בקרב כל העובדים. במסמך מדיניות אבטחת מידע טיפוסי נהוג להעלות, בין היתר, את הנושאים הבאים:

- אבטחת מידע בניהול משאבי אנוש
- אבטחה פיזית וסביבתית
- ניהול תקשורת ותפעול
- קיום בקרות גישה לוגיות
- ניהול סיסמאות
- קיום בקרות ומנגנוני הצפנה
- פיתוח ותחזוקה של מערכות
- המשכיות עסקית

5.2. **בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות אשר מפרט כיצד על המחלקה ועל המשתמשים בעירייה להתנהל בתחום המיחשוב בכלל ובתחום אבטחת המידע בפרט.**

5.3. בהתאם לסעיף 3(2) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017

" הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר".

5.4. **בביקורת נמצא כי הממונה על אבטחת מידע לא הכין נוהל אבטחת מידע ולפיכך גם הנוהל לא אושר בעירייה. על הנוהל לכלול בין היתר את הפרטים הבאים:**

5.4.1. **הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר כאמור בתקנה 6;**

5.4.2. **הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8;**

5.4.3. **תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;**

5.4.4. **הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;**

5.4.5. **הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5)א(, אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;**

5.4.6. **אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11 , לפי חומרת האירוע ומידת רגישות המידע;**

5.4.7. **הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12 .**

5.5. בהתאם לסעיף 3(3) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

"הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו"

5.6. **בביקורת נמצא כי הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת.**

5.7. בהתאם לסעיף 5(א) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 על מנהל מאגר המידע לבצע מיפוי מערכות המאגר וביצוע סקר סיכונים. הסעיף קובע כי:

"בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה:

(1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;

(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;

(4) תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;

(5) תאריך העדכון האחרון של המסמך ושל רשימת המצאי."

5.8. **בביקורת נמצא כי לא בוצע מיפוי וסקר סיכונים.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

6. <u>טיפול באירועי אבטחת מידע</u>

6.1. **"אירוע אבטחת מידע"** – הוא כל מקרה בו קיים חשד לפגיעה בסודיות, אמינות או זמינות במערכות העירייה, מידע העירייה או כל אמצעי אחר אשר שייך לעירייה.

6.2. לטיפול באירועי אבטחת מידע חשיבות רבה, במספר מישורים: מניעה, תגובה בזמן אמת, ותחקור אירועים לצורך הפקת לקחים.

6.3. אירועי אבטחת מידע יכולים לכלול תקיפה מכוונת על מערכות העירייה הן על ידי גורמים חיצוניים והן על ידי גורמים פנימיים וכן נזקים הנגרמים מרשלנות או טעויות.

6.4. נוהל מס' 8 קובע כי "כל מקרה של אירוע אבטחתי חריג ייחקר – מטרת התחקיר הסקת מסקנות כדי למנוע אירוע כזה בעתיד".

6.5. **לא קיים נוהל עירייה פנימי אשר מנחה מהו הטיפול הנדרש באירועי אבטחת מידע.**

6.6. **לא קיים תיעוד כלשהו באשר לאירועי אבטחת מידע שהתרחשו (אם התרחשו) במהלך השנים בעירייה.**

6.7. **לא קיימים בעירייה כלי ניטור על פעילות המשתמשים. לדוגמא, משתמשים אשר מתחברים שלא בשעות העבודה, משתמשים שטועים בסיסמא שלהם ולפיכך מתנתקים, משתמשים שמנקודת התקשורת שלהם מתחבר מחשב שאינו מחשב של העירייה וכיו"ב.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

7. ניהול מאגרי המידע

7.1. בסעיף 8 לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

8 (א) לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:
(1) המאגר נרשם בפנקס ;
(2) הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב1) ;
(3) המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

7.2. הביקורת מציינת כי מטרת רישום המאגר היא להבטיח את ההגנה על הפרטיות במאגרי מידע, ולתת כלים, הן בידי רשם מאגרי המידע, והן בידי הציבור שמידע עליו מנוהל במאגרי המידע, לאכוף את הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי מאגרים.

7.3. **מבדיקת הביקורת עולה כי כל מאגרי המידע הקיימים בעירייה מנוהלים בעירייה ללא שנרשמו בפנקס אצל רשם מאגרי המידע, במשרד המשפטים.**

8. הגשת בקשה לרישום מאגר מידע לרשם

8.1. בהתאם לסעיף 9 (א) – 9(ב) לחוק הגנת הפרטיות , תשמ"א – 1981 נקבע כי:

בקשה לרישום מאגר מידע תוגש לרשם.
(ב) בקשה לרישום מאגר מידע תפרט את –
(1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל ;
(2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע ;
(3) סוגי המידע שייכללו במאגר ;
(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה ;
(5) פרטים בדבר קבלת מידע, דרך קבע, מגוף ציבורי כהגדרתו בסעיף 23, שם הגוף הציבורי מוסר המידע ומהות המידע הנמסר, למעט פרטים הנמסרים בהסכמת מי שהמידע על אודותיו.

8.2. **כאמור בסעיף 7 לדוח ביקורת זה, העירייה לא רשמה את מאגרי המידע ברשם מאגרי המידע ולפיכך , גם לא הגישה בקשה לרישום המאגרים בהתאם להוראות סעיף 9 לחוק הגנת הפרטיות.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

9. <u>בעל הרשאה</u>

9.1. בהתאם לסעיף 1 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

"בעל הרשאה" - יחיד אשר יש לו גישה לאחד מאלה על פי הרשאתו של בעל המאגר או המחזיק:
(1) מידע מהמאגר;
(2) מערכות המאגר;
(3) מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו.
על אף האמור, מחזיק שאינו יחיד או יחיד שקיבל גישה על פי הרשאה של מחזיק, לא ייחשב כבעל הרשאה של בעל המאגר;

9.2. עיריית קריית ביאליק מאפשרת למספר חברות העובדות עם העירייה ומאפשרת להם גישה למאגרי מידע הקיימות בעירייה לצורך עבודתן.

9.3. **נמצא כי ב 7 – מתוך 10 החברות החיצוניות שעובדות עם העירייה ושקיבלו הרשאה להחזיק במידע לא חתמו על הסכם סודיות.**

9.4. **כמו כן נמצא כי 5 מתוך 10 החברות שנבדקו , לא נחתם כלל הסכם התקשרות בין החברה לעירייה.**

9.5. בהתאם לסעיף 2 (א) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר (להלן - מסמך הגדרות המאגר), את כל העניינים האלה לפחות:
(1) תיאור כללי של פעולות האיסוף והשימוש במידע;
(2) תיאור מטרות השימוש במידע;
(3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה;
(4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;
(5) פעולות עיבוד מידע באמצעות מחזיק;
(6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;
(7) שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה.

9.6. **נמצא כי העירייה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך הגדילה את הסיכוי לפגיעה במאגרי המידע העירוניים.**

9.7. **הביקורת ביצעה בדיקה באם חברות אלו חתומות על מסמך הגדרות כאמור בתקנות (ראה טבלה מסכמת בהערה 10.3 לדוח זה)**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

10. <u>מיקור חוץ</u>

10.1. בהתאם לסעיף 15 (א) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017:

"בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע –
(1) יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות;
(2) יקבע במפורש בהסכם עם הגורם החיצוני(בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה (1):
(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי התקשרות;
(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;
(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;
(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;
(ה) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;
(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);
(ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף - חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;
(ח) 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;
(3) יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה (2(א)) עד (ה), וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו;
(4) ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1)."

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

10.2. **מבדיקת הביקורת עולה כי העירייה התקשרה עם מספר גורמים חיצוניים לצורך קבלת שירות ובהתאם לטבלה האמורה:**

מס"ד	שם הגורם החיצוני	מחלקה	מאגרים	האם בוצעה בטרם ההתקשרות סיכוני אבטחת המידע
1	מטרופולינט	גביה הנהלת חשבונות רכש פיקוח עירוני רווחה חינוך וגני ילדים	ארנונה, שילוט, מרשם אוכלוסין (מימד), מאגר ספקים, מטופלי רווחה, דוחות חנייה, רישום תלמידים וילדים, מערכת ניהול כספים של החינוך	כן
2	זיצר	גביה, הנהלת חשבונות, רכש, חינוך	מאגר ספקים, ארנונה, שילוט, מרשם אוכלוסין,	לא*
3	מגע"ר	גביה, פיקוח עירוני,	ארנונה, שילוט, מרשם אוכלוסין, דוחות חנייה	כן
4	אוטומציה,	משאבי אנוש ושכר	משכורות עובדים, פרטי עובדים וגמלאים	כן
5	סינאל	משאבי אנוש ושכר	משכורות עובדים, פרטי עובדים וגמלאים	לא
6	רמה מערכות	רישוי עסקים	מעקב אחר רישיונות עסק לעסקים בעיר	לא
7	סורין הרשקו	וטרינר עירוני	ניהול פרטי מחזיקי בעלי הכלבים המחוסנים ב- 3 רשויות	לא
8	כרמל	חברת קדישא	מאגר נפטרים	לא
9	Expo	מרכז הספורט "אפק"	ניהול רשימת מנויים	לא
10	אגרון פלוס	ספרייה עירונית	מנויי ספרייה	לא

* במסגרת ההסכם לא נחתם התחייבות לשמירת סודיות.

10.2.1. **מהטבלה האמרה עולה כי 7 מתוך 10 החברות לא חתמו על טופס התחייבות לשמירת סודיות וכן בטרם ביצוע ההתקשרות לא בוצע סקר סיכונים לצורך אבטחת המידע.**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

.10.3 **<u>בטבלה האמורה בוצעה בדיקה באם במסגרת ההסכם עם הגורמים החיצוניים נכללו הסיכונים הבאים:</u>**

	מטרופ ולינט	זיצר	מגע"ר	אוטו מציה	סינאל	רמה מערכות	סורין הרשקו	כר מל	Ex po	אגרון פלוס
רישום המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי התקשרות	כן	**לא**	כן	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
רישום מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן	כן	**לא**	כן	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
רישום סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות	כן	**לא**	כן	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
אופן השבת המידע לידי העירייה בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע	כן	**לא**	לא	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
יישום הנחיות בתחום אבטחת המידע שהגורם החיצוני חייב בהן כפי שנקבעו ע"י העירייה	כן	**לא**	כן	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
האם הגורם החיצוני החתים את בעלי ההרשאות בחברתו על התחייבות לשמור על סודיות המידע, ולכבד את ההסכם ולפעול בהתאם לדרישות אבטחת המידע של העירייה	כן	**לא**	כן	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**
האם הגורם החיצוני מחויב לדווח אחת לשנה על אודות אופן ביצוע חובותיו בהסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה	כן	**לא**	**לא**	**כן**	**לא**	**לא**	**לא**	**לא**	**לא**	**לא**

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

11. <u>ההיבט האזרחי, הפלילי והעונשי</u>

11.1. במהלך הביקורת נשאלה הביקורת, **מה קורה אם לא רושמים מאגר מידע שחלה עליו חובת רישום?**

11.1.1. אין לנהל או להחזיק מאגר מידע מאגר מידע החייב ברישום מבלי שנרשם. ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה פלילית שדינה מאסר שנה, לפי סעיף 31א(א)(1) לחוק הגנת הפרטיות.

11.1.2. בנוסף, ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה בגינה רשאי רשם מאגרי מידע להטיל קנס מינהלי (ר' לעניין זה את תקנות העבירות המינהליות (קנס מינהלי - הגנת הפרטיות), התשס"ד-2004).

11.1.3. פגיעה בפרטיות של אדם היא עוולה כמו כל עוולה אחרת עפ"י דיני הנזיקין. כלומר, אדם שחושב שנגרם לו נזק עקב אי הקפדה על השימוש הנאות במידה אודותיו, רשאי לתבוע את המזיק את נזקיו בתביעה אזרחית לפיצויים אזרחיים.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

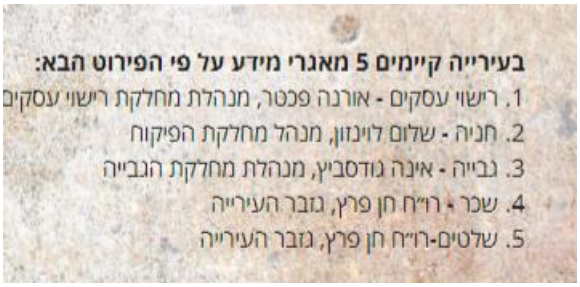
סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

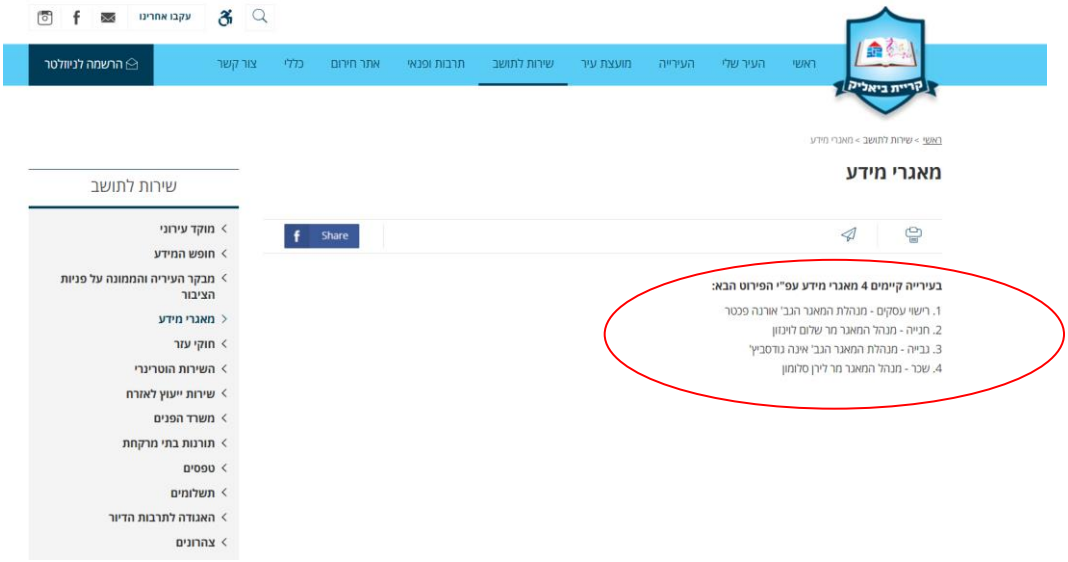
12. <u>שקיפות</u>

12.1. מדוח לתושב לשנת 2015 שפורסם באתר העירייה עולה כי בעירייה ישנם 5 מאגרי מידע (להלן צילום מסך של דוח לתושב).

12.2. באתר העירייה פורסם כי ישנם 4 מאגרי מידע (רצ"ב צילום מסך מתוך אתר העירייה).

12.3. **בבדיקתנו עלה כי בעירייה ישנם 11 מאגרי מידע ולכן הביקורת מעירה כי יש לפרסם באתר העירייה ובדוח לתושב את כלל מאגרי המידע הקיימים.**





תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

סיכום והמלצות

1. רקע

1.1. הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל. עניינה של הזכות לפרטיות הוא בשמירה על האוטונומיה של האדם, בשמירה על צנעת חייו ועניינו האישיים ואף בהגנה על האדם מפני שימוש לרעה במידע על אודותיו. מידע פרטי הוא בעל ערך רב, לרבות ערך כלכלי, ולכן לחברות מסחריות ולגופים אחרים אינטרס ברור באיסופו ובשמירתו במאגרי מידע. מאגרי מידע מסכנים בעצם קיומם את הפרטיות, ועל כן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע הנאגר בו.

1.2. איסוף המידע כיום פשוט מבעבר, וניתן לאסוף מידע על אדם אגב שימוש שהוא עושה בשירותים רבים, בעת חקיקתו, נועד חוק הגנת הפרטיות להתמודד עם מציאות של מאות מאגרי מידע שחייבים ברישום בשנת 1981 נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), במטרה "לשריין את ההגנה של האדם לזכותו לפרטיות".

1.3. פעולתם של גופים ציבוריים מושתתת על מערכות מידע הכוללות נתונים רבים על התושבים מעמד אישי, מצב בריאות, מצב כלכלי, הכשרה מקצועית, דעות ואמונות שחשיפתם עלולה לפגוע בפרטיותם של התושבים.

1.4. בעירייה פועלות מערכות מידע ממוחשבות רבות החיוניות להבטחת תקינות פעילותה השוטפת בתחומים האלה: כספים (גבייה, שכר, תשלומים לספקים ועוד); תכנון ובנייה; חינוך (שירות פסיכולוגי חינוכי, גני ילדים, קייטנות ועוד); רווחה; כוח אדם; רישוי עסקים; תחבורה וחניה; תברואה ועוד. מאגרים אלה הם הבסיס לעבודתם של הרשויות. בעירייה ישנם 11 מאגרי מידע, בהתאם לפירוט המחלקות הבאות: גביה, הנהלת חשבונות ורכש, משאבי אנוש ושכר, חינוך וגני ילדים, פיקוח עירוני, רישוי עסקים, ווטרינר עירוני, רווחה, חברת קדישא, מרכז הספורט וספריה עירונית.

1.5. יחידת מערכות המידע בעירייה אמונה על מתן שירותי מחשב לעובדי העירייה, ניהול המשתמשים, אבטחת המידע ותפעול שוטף של מערכות המחשב בעירייה. היחידה מטפלת בכ- 2,000 מחשבים / שרתים. לצורך ביצוע חלק ממשימותיהם, על היחידה לעבור פיזית בין אתרים שונים בהם נמצאים מחשבי ושרתי העירייה.

1.6. במהלך החודשים מרץ ועד אוקטובר 2017 בוצעה ביקורת בעיריית קריית ביאליק.

1.7. הביקורת בוצעה בהתאם לתוכנית העבודה של מבקר העירייה לשנת 2017. הנושא נכלל בתכנית העבודה השנתית, בשל דרישת ראש העיר ובהתאם לסמכותו בחוק. הביקורת הסתמכה על הוראות החוק כפי שמופיעות בסעיף 3 בדו"ח זה.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

2. <u>פרק 2 - מנהל אבטחת מידע</u>

2.1. נמצא כי העירייה מינתה עובד ייעודי העוסק בתחום אבטחת המידע, אולם לא מונה כמפקח האחראי על תחום מאגרי המידע.

3. <u>פרק 3 - מבנה ארגוני</u>

3.1. נמצא כי בניגוד להנחיות אגף משאבי אנוש במשרד הפנים הקובעות כי המנמ"ר יהיה כפוף מנהלתית למנכ"ל העירייה, המנמ"ר כפוף לגזבר העירייה.

4. <u>פרק 4 - ועדת היגוי לאבטחת מידע</u>

4.1. לא קיים בעירייה נוהל העוסק בפעילות וועדת היגוי לאבטחת מידע.

4.2. לא קיימת בעירייה וועדת היגוי לאבטחת מידע, וממילא לא מתכנסת וועדה, כנדרש בנוהל מסגרת מס' 5 (פירוט בהרחבה נמצא בדוח המלא).

5. <u>פרק 5 - מדיניות אבטחת מידע ותכנית עבודה</u>

5.1. בניגוד לנוהל המסגרת, לא קיים במחלקה מסמך מדיניות אשר מפרט כיצד על המחלקה ועל המשתמשים בעירייה להתנהל בתחום המיחשוב בכלל ובתחום אבטחת המידע בפרט.

5.2. הממונה על אבטחת מידע לא הכין נוהל אבטחת מידע ולפיכך גם הנוהל לא אושר בעירייה. על הנוהל לכלול בין היתר את הפרטים הבאים:

5.2.1. הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר כאמור בתקנה 6;

5.2.2. הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8;

5.2.3. תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;

5.2.4. הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;

5.2.5. הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5)א(, אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;

5.2.6. אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11 , לפי חומרת האירוע ומידת רגישות המידע;

5.2.7. הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12 .

5.3. הממונה על אבטחת מידע לא הכין תכנית לבקרה שוטפת.

5.4. בביקורת נמצא כי לא בוצע מיפוי וסקר סיכונים, בהתאם לסעיף 5(א) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

6. <u>פרק 6 - טיפול באירועי אבטחת מידע</u>

6.1. לא קיים נוהל עירייה פנימי אשר מנחה מהו הטיפול הנדרש באירועי אבטחת מידע.

6.2. לא קיים תיעוד כלשהו באשר לאירועי אבטחת מידע שהתרחשו (אם התרחשו) במהלך השנים בעירייה.

6.3. לא קיימים בעירייה כלי ניטור על פעילות המשתמשים. לדוגמא, משתמשים אשר מתחברים שלא בשעות העבודה, משתמשים שטועים בסיסמא שלהם ולפיכך מתנתקים, משתמשים שמנקודת התקשורת שלהם מתחבר מחשב שאינו מחשב של העירייה וכיו"ב.

7. <u>פרק 7 - ניהול מאגרי המידע</u>

7.1. מבדיקת הביקורת עולה כי כל מאגרי המידע הקיימים בעירייה מנוהלים בעירייה ללא שנרשמו בפנקס אצל רשם מאגרי המידע, במשרד המשפטים.

8. <u>פרק 8 - הגשת בקשה לרישום מאגר מידע לרשם</u>

8.1. העירייה לא רשמה את מאגרי המידע ברשם מאגרי המידע ולפיכך , גם לא הגישה בקשה לרישום המאגרים בהתאם להוראות סעיף 9 לחוק הגנת הפרטיות.

9. <u>פרק 9 - בעל הרשאה</u>

9.1. נמצא כי ב 7 – מתוך 10 החברות החיצוניות שעובדות עם העירייה ושקיבלו הרשאה להחזיק במידע לא חתמו על הסכם סודיות.

9.2. ב- 5 מתוך 10 החברות שנבדקו , לא נחתם כלל הסכם התקשרות בין החברה לעירייה.

9.3. העירייה לא הגדירה לבעלי ההרשאה מסמך הגדרות ובכך הגדילה את הסיכוי לפגיעה במאגרי המידע העירוניים.

10. <u>פרק 10 - מיקור חוץ</u>

10.1. ב- 7 מתוך 10 החברות שנבדקו נמצא כי החברות לא חתמו על טופס התחייבות לשמירת סודיות וכן בטרם ביצוע ההתקשרות לא בוצע סקר סיכונים לצורך אבטחת המידע.

11. <u>פרק 11 – ההיבט האזרחי, הפלילי והעונשי</u>

11.1. אי רישום של מאגר מידע החייב ברישום מבלי שנרשם, מהווה עבירה פלילית שדינה מאסר שנה, לפי סעיף 31א(א)(1) לחוק הגנת הפרטיות.

11.2. בנוסף, ניהול, החזקה או שימוש במאגר מידע שחייב ברישום ולא נרשם מהווה עבירה בגינה רשאי רשם מאגרי מידע להטיל קנס מינהלי (ר' לעניין זה את תקנות העבירות המינהליות (קנס מינהלי - הגנת הפרטיות), התשס"ד-2004).

11.3. פגיעה בפרטיות של אדם היא עוולה כמו כל עוולה אחרת עפ"י דיני הנזיקין. כלומר, אדם שחושב שנגרם לו נזק עקב אי הקפדה על השימוש הנאות במידה אודותיו, רשאי לתבוע את המזיק את נזקיו בתביעה אזרחית לפיצויים אזרחיים.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."

12. <u>פרק 12 – שקיפות</u>

בעירייה ישנם 11 מאגרי מידע, אולם בדוח לתושב נרשם כי ישנם 4 מאגרי מידע ובאתר האינטרנט העירוני נרשם כי ישנם 5 מאגרי מידע ולכן הביקורת מעירה כי יש לפרסם באתר העירייה ובדוח לתושב את כלל מאגרי המידע הקיימים.

תשומת לב הקורא להוראות פקודת העיריות (נוסח חדש) תשכ"ד 1964 לגבי תוכן מסמך זה:-

- **סעיף 170ג.(ו)** " לא יפרסם אדם דוח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העירייה, ואולם מבקר העירייה או ראש העירייה רשאי, באישור הועדה, להתיר פרסום כאמור."

סעיף 334א. " המפרסם דוח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג.(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו- מאסר שנה."