המועצה האזורית לכיש

מבקר וממונה תלונות ציבור

אחועם
אלישא
אמציה
בני-
עקלים
גוהה
יפ נתן
כפאי
קטוף
לכיש
מנוחה
נהופה
נוצה
עץ
ניר ח"ן
שדמ
שדה
צוף
שדה
משה
שחף
שקף
תלמים

לכבוד

מר דני מורביה - ראש המועצה

וחברי המליאה

שלום וברכה,

הנדון: <u>דוח ביקורת לשנת 2022</u>

הריני מתכבד להגיש לכם את דוח הביקורת לשנת 2022.

1. ראשית – תודה. תודה על שיתוף הפעולה המלא מכל בעלי התפקידים אותם פגשתי. כולם סייעו להבאת נתונים והיו נכונים לסייע לכל הדרוש.

2. הדוח עוסק בנושאים הבאים:

א. אבטחת מידע ושמירה על הפרטיות

1. מבוא, דיון כללי ומישור נורמטיבי

2. מסמך הגדרות מאגר

3. רישום מאגרי מידע

4. חובת מבקש מידע, זכות העיון ותיקון מידע

5. נהלי אבטחת מידע

6. מסירת מידע או ידיעות מאת גופים ציבוריים

7. ועדת היגוי לתחום אבטחת המידע

8. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב

9. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות

10. **תקצוב אבטחת מידע**
11. **הדרכה וקיום אבטחת מידע אצל עובדים**
12. **חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת**
13. **שמירה, גיבוי ושחזור של נתוני אבטחה**
14. **רישוי תוכנות**
15. **אבטחה פיזית וסביבתית**
16. **ניהול הרשאות גישה וזיהוי ואימות**
17. **חיבור התקנים**
18. **בקרה ותיעוד גישה**
19. **תיעוד של אירועי אבטחה**
20. **עיר חכמה**
21. **מיקור חוץ**
22. **מינוי ממונה אבטחת מידע**
23. **מינוי ממונה הגנה על הפרטיות**

ב. **ועדת הביקורת ביישובים**

ג. **תיקון ליקויים מדוחות קודמים**

1. **הסעות תלמידים**
   - **בדיקת נכונות שיעורי השתתפות**
   - **איחוד מסלולים והתייעלות**
   - **מנגנון הקנסות**
   - **נתוני התלמידים**
   - **נהלים**
   - **הסכמים**
   - **תחום הליווי בחינוך המיוחד**
   - **בטיחות**
   - **פניות תושבים**
   - **תחנות ההסעה**
   - **הסעת תלמידים ללא שימוש בחגורות בטיחות ובעמידה**
2. **פסולת נהורה**
3. **דוח ביקורת משרד הפנים**

3. ראש המועצה העביר את הערותיו לדוח והן משולבות בו.
4. הוועדה לענייני ביקורת דנה בדוח ובהערות ראש המועצה ומבקשת את אישור המועצה לדוח ולסיכום הוועדה.

5. בהתאם לחוק, תוך חודשיים מהיום שהגישה הוועדה את סיכומיה והצעותיה, תקיים המועצה דיון מיוחד בהם ובדוח המבקר ותחליט בדבר אישור הסיכומים או ההצעות כאמור.

6. לפי סעיף 170ג. החל על מועצות אזוריות:

(א) המבקר יגיש לראש המועצה דוח על ממצאי הביקורת שערך; הדוח יוגש אחת לשנה, לא יאוחר מ-1 באפריל של השנה שלאחר השנה שלגביה הוגש הדוח; בדוח יסכם המבקר את פעולותיו, יפרט את הליקויים שמצא וימליץ על תיקון הליקויים ומניעת הישנותם בעתיד; בעת הגשת הדוח לפי סעיף קטן זה, ימציא המבקר העתק ממנו לועדה לעניני ביקורת;

(ב) בנוסף לאמור בסעיף קטן (א) רשאי המבקר להגיש לראש המועצה ולועדה לעניני ביקורת דו"ח על ממצאי ביקורת שערך בכל עת שייראה לו או כאשר ראש המועצה או הועדה לעניני ביקורת דרשו ממנו לעשות כן.

(ג) תוך שלושה חדשים מיום קבלת דו"ח המבקר, יגיש ראש המועצה לועדה לעניני ביקורת את הערותיו על הדו"ח וימציא לכל חברי המועצה העתק מהדו"ח בצירוף הערותיו.

(ד) הועדה לעניני ביקורת תדון בדו"ח המבקר ובהערות ראש המועצה עליו ותגיש למועצה לאישור את סיכומיה והצעותיה תוך חדשיים מיום שנמסרו לה הערות ראש המועצה כאמור בסעיף קטן (ג); לא הגיש ראש המועצה את הערותיו על הדוח עד תום התקופה האמורה, תדון הועדה בדוח המבקר ותגיש למועצה לאישור את סיכומיה והצעותיה עד תום חמישה חודשים ממועד המצאתו על ידי מבקר המועצה לועדה; בטרם תשלים הועדה את סיכומיה והצעותיה רשאית היא, אם ראתה צורך בכך, לזמן לדיוניה נושאי משרה של המועצה או של גוף רשותי מבוקר כדי לאפשר להם להגיב על הדו"ח.

(ה) (1) תוך חדשיים מן היום שהגישה הועדה את סיכומיה והצעותיה תקיים המועצה דיון מיוחד בהם ובדוח המבקר ותחליט בדבר אישור הסיכומים או ההצעות כאמור;

(2) לא הגישה הועדה את סיכומיה והצעותיה לחברי המועצה עד תום התקופה כאמור בסעיף קטן (ד), או לא המציא ראש המועצה לכל חברי המועצה העתק מהדוח בצירוף הערותיו, ימציא המבקר עותק הדוח לכל חברי המועצה והמועצה תדון בדוח ובהמלצותיו לא יאוחר משבעה חודשים ממועד הגשתו לראש המועצה.

7. לידיעתכם, לפי סעיף 170גו לפקודת העיריות החל על מועצה אזורית, לא יפרסם אדם דו״ח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר המועצה, ואולם מבקר המועצה או ראש המועצה רשאי, באישור הועדה, להתיר פרסום כאמור. לפי סעיף 334א. לפקודת העיריות החל על המועצה האזורית, המפרסם דו״ח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו – מאסר שנה.

הביקורת נועדה להביא לידי שיפור, תועלת והמשך עשיה ברוכה ונכונה לצורך השגת מטרות הארגון תוך קיום הדין.

דלתי פתוחה תמיד לשמיעת הערות והארות לשיפור ביקורת אפקטיבית.

נהורה

טבת התשפ״ג (ינואר 2023)

בברכת הצלחה,

שלמה מאיר רבינוביץ, עו״ד

מבקר המועצה

פרק א' - מבוא 8

אבטחת המידע ושמירת הפרטיות ברשויות המקומיות 8

הצורך באבטחת המידע ושמירת הפרטיות במועצה האזורית לכיש 10

פרק ב' - על הפרטיות ואבטחת המידע - המישור הנורמטיבי 11

כללי 11

פרטיות במועצה האזורית 28

פרק ג' – מטרות, היקף הביקורת, מתודולוגיה.....37

מטרות הביקורת 37

היקף הביקורת 37

מתודולוגיה – שיטת הביקורת 39

פרק ד' ממצאים והמלצות.....39

מידע כללי 39

סקר מקצועי למיפוי מחשוב, רשת, ורישוי..... 40

פירוט הממצאים וההמלצות..... 40

1. מסמך הגדרות מאגר 40

2. רישום מאגרי מידע 42

3. חובת מבקש מידע, זכות העיון ותיקון מידע 44

4. נהלי אבטחת מידע 47

5. מסירת מידע או ידיעות מאת גופים ציבוריים..... 50

6. ועדת היגוי לתחום אבטחת המידע..... 53

7. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב..... 55

8. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות..... 56

9. תקצוב אבטחת מידע..... 59

10. הדרכה וקיום אבטחת מידע אצל עובדים..... 60

11. חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת 64

12. שמירה, גיבוי ושחזור של נתוני אבטחה..... 66

13. רישוי תוכנות..... 67

14. אבטחה פיזית וסביבתית 68

15. ניהול הרשאות גישה וזיהוי ואימות..... 72

16. חיבור התקנים 73

17. בקרה ותיעוד גישה 74

18. תיעוד של אירועי אבטחה..... 75

19. עיר חכמה 76

20. מיקור חוץ 78
21. מינוי ממונה אבטחת מידע 82
22. מינוי ממונה הגנה על הפרטיות 85
פרק ה' - סיכום ומסקנות 89
ריכוז הממצאים וההמלצות – אבטחת מידע והגנת הפרטיות 92
1. מסמך הגדרות מאגר 92
2. רישום מאגרי מידע 92
3. חובת מבקש מידע, זכות העיון ותיקון מידע 93
4. נהלי אבטחת מידע 94
5. מסירת מידע או ידיעות מאת גופים ציבוריים 95
6. ועדת היגוי לתחום אבטחת המידע 95
7. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב 96
8. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות 97
9. תקצוב אבטחת מידע 98
10. הדרכה וקיום אבטחת מידע אצל עובדים 98
11. חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת 99
12. שמירה, גיבוי ושחזור של נתוני אבטחה 100
13. רישוי תוכנות 100
14. אבטחה פיזית וסביבתית 101
15. ניהול הרשאות גישה וזיהוי ואימות 101
16. חיבור התקנים 102
17. בקרה ותיעוד גישה 102
18. תיעוד של אירועי אבטחה 103
19. עיר חכמה 103
20. מיקור חוץ 104
21. מינוי ממונה אבטחת מידע 106
22. מינוי ממונה הגנה על הפרטיות 106
ועדת הביקורת ביישובים 108
תיקון ליקויים מדוחות קודמים 110
הסעות תלמידים 111
בדיקת נכונות שיעורי השתתפות 111
איחוד מסלולים והתייעלות 112
מנגנון הקנסות 112
נתוני התלמידים 113
נהלים 114
הסכמים 114

תחום הליווי בחינוך המיוחד 116
בטיחות 118
פניות תושבים 122
תחנות ההסעה 135
הסעת תלמידים ללא שימוש בחגורות בטיחות ובעמידה 138
פסולת נהורה 139
140
דוח ביקורת משרד הפנים 141
הערות ראש המועצה 142
נספח א' 146
נספח ב' 183
נספח ג' 209

אבטחת המידע ושמירת הפרטיות ברשויות המקומיות

1. הרשות המקומית מספקת שירותים במגוון תחומים בממשק ישיר לחיי התושבים כחינוך, בריאות, רווחה, איכות הסביבה, פיתוח פיסי וחברתי, תרבות וביטחון אישי.
2. הרשות מקומית הינה "גוף ציבורי" המחויב לשמר את יחסי האמון בינה לבין התושב, והיא כפופה להוראות חוק המגבירות את האחריות בתחומים שונים וכך גם להוראות בתחום הפרטיות.
3. מספר ה"ערים החכמות" (במאפיינים ובגוונים שונים) הולך וגדל משנה לשנה[1], והן עושות שימוש בטכנולוגיות מידע ותקשורת לשיפור הניהול והשירות שניתן לתושבים. באופן זה, ועם השימוש ההולך וגובר בטכנולוגיות מגוונות, כמות הנתונים שבידי הרשויות המקומיות הולכת וגדלה. מכך ברור, כי פגיעה במערכות הטכנולוגיות של הרשויות המקומיות, עלולה לגרום לנזקים כבדים, וביניהם פגיעה בהתנהלות הרשות, פגיעה בשירותים הניתנים לתושבים ופגיעה בצנעת הפרט.
4. במסגרת עבודת הרשות, מצטבר מידע הכולל, בין היתר, נתונים על אישיותו של אדם, מעמדו האישי, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו אמונתו וכן "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות" – מצ"ב כ**נספח א'**) כגון אבחונים פסיכולוגיים, חוות דעת של פסיכולוגים, עובדים סוציאליים ועוד.
5. ברשות המקומית קיימים מאגרי מידע בתחומים שונים ובין היתר בתחומים הבאים: רישוי עסקים, תחבורה וחניה, תברואה, כספים, תכנון ובנייה, חינוך, רווחה וכוח אדם.
6. המידע, הכולל נתונים רבים על התושבים, נאסף בידי הרשות ומשמש בסיס לעבודתה.
7. בנוסף לכך, בידי הרשות קיים מידע הנוגע לעבודה השוטפת שלה - גם בלי קשר ישיר למידע בדבר התושבים עצמם - כגון מידע הנוגע לעובדי המועצה, עובדים פוטנציאליים, ספקים וספקים פוטנציאליים, הצעות למכרזים ועוד.
8. החזקת מאגרי המידע מעלה חששות שונים כגון חשש משימוש חורג ממטרת איסוף המידע המקורית, חשש לחשיפת מידע לא מוצדקת לנותני שירותים חיצוניים ומהם הלאה ועוד.
9. מאגרי המידע של הרשות מכילים פרטים אישיים וסודיים רבים, ולכן פגיעה בנתוני הרשויות המקומיות ובמידע האצור בהן או חשיפתם, עלולה לפגוע בפרטיות ולהסב נזקים שונים.
10. הנה כי כן, פעילות הרשות המקומית חשופה לסיכונים לפרטיות הנובעים מניהול והחזקת מידע רחב ורגיש.
11. התלות של הרשות המקומית כמו של ארגונים רבים אחרים במערכות הממוחשבות שלהם, הולכת וגדלה ועימה הצורך בהגנה על מרחב הסייבר2.

---

1 בהחלטת ממשלה מספר 2733 של ממשלת ישראל מיום 11.06.2017 אושרה התוכנית הדיגיטלית הלאומית, קידום המיזם הלאומי "ישראל דיגיטלית" ובכללה החלטה על גיבוש תוכנית לקידום תחום הערים החכמות בישראל.

2 מרחב הסייבר מורכב בעיקר מהגורמים הבאים: מערכות ממוכנות ממוחשבות, תוכנות, רשתות מחשוב ותקשורת, מידע ממוחשב, תוכן בתעבורה, נתוני תעבורה ובקרה והמשתמשים עצמם. יש שיסבירו, ש"אבטחת מידע" היא שם כולל להגנה על נתונים ו"אבטחת סייבר" היא שם כולל להגנה על נתונים ממרחב הסייבר. שניהם עוסקים בהגנה על מידע ומערכות מידע ומטרתם לספק סודיות, שלמות וזמינות

12. האירועים אשר מתרחשים במרחב הסייבר הכלל-עולמי ובישראל, מלמדים על מגמת עלייה באיומי פגיעה, במספר האירועים והתקיפות וכן בחומרתם ומורכבותם.
13. פגיעה במרחב הסייבר עלולה להסב נזקים כבדים לצנעת הפרט, למסחר, לתקינות וליעילות התפקודית, הארגונית והניהולית.
14. אבטחת המידע נועדה להגן מפני גישה, שימוש, חשיפה, ציתות, העתקה, השמדה וכל שיבוש או תקלה של מידע ומערכות מידע מגורמים שאינם מורשים, בזדון או בשגגה ומכוונת בעיקר להשגת המטרות הבאות:

- **זמינות** - (availability) - שמירה על זמינות ויעילות הגישה אל המידע. לדוגמה, נזק עלול להיגרם בתקיפת סייבר, הגורמת לכך שהמידע אינו זמין לחברה או ללקוחותיה בעת נפילת אתר ודרישת כופרה וכדו'.
- **אמינות (מהימנות) / שלמות** - (integrity) ואמינות - הגנה משינוי זדוני או לא מכוון של המידע או השמדתו, כולל הבטחת אי התכחשות ואימות זהות בעל המידע. לדוגמה, נזק עלול להיגרם בתקיפת סייבר הפוגעת בדוחות תאגיד, כך שלא ייצג את מצבו האמיתי, או תקיפה המשבשת את תפקודו התקין של מפעל / חברה.
- **סודיות** - (confidentiality) - הגבלת גישה או חשיפה לא מורשית של מידע, כולל הגנה על פרטיות וזכויות קנייניות במידע או הנובע ממנו. כגון תקיפת סייבר לצורך הדלפת פרטי לקוחות או סוד מסחרי אל האינטרנט.

15. אבטחת מידע מתבצעת בכמה תחומים: **אבטחה פיזית** - ביצוע פעולות בחומרה ובתשתיות; **אבטחה לוגית** – כמו: הפעלת מנגנוני תוכנה ייעודיים, הרשאות, הזדהות, הצפנה, הגנה מפני תוכנות מזיקות, גיבוי; **אבטחה פיזית של מידע לא ממוחשב** - כל הפעולות הנדרשות להגנה על פלטי מחשב, על דוחות, על מזכרים ועל מסמכים שונים המכילים מידע כהגדרתו בחוק.
16. **על קצה המזלג - מונחי היסוד בתחום**[3]:

16.1. אבטחה פיזית

א. אבטחה פיזית של מערכות מידע הינה "מכלול השיטות, אמצעי הגנה פיזיים ונהלים, שמטרתם למדר את מערכות המידע ולהגן פיזית על אזור מוגדר כדי לאפשר גישה לאזור זה או למנוע אותה, לפי הצורך, וכן להגן על הנכסים הנמצאים בו מפני השמדה, השחתה או גניבה".[4]

ב. האבטחה הפיזית כוללת, בין השאר, טיפול בסיכוני אש, עשן, רעידות אדמה, חשמל ומים בעיקר בחדרי שרתים וחדרי המחשב; הגנה מפגיעה במערכות המחשוב כגון נפילת מתח, ניתוק תקשורת וכדו', הגנה מפני גניבה, השחתה וחבלה; ניהול ואבטחה של אמצעי אחסון מגנטיים ואופטיים; אבטחת רשומות ותעודות רשמיות; ניהול מלאי חמרה ותכנה טיפול במסמכי קלט ופלט; העברת מידע והוצאתו; רישום מאגרי מידע; שימור רשומות אלקטרוניות.

16.2. אבטחה לוגית

של המידע ללא תלות בסוג המידע או באופן האחסון. בדוח זה, הביטוי "אבטחת מידע" ישמש למכלול ההגנה על הנתונים.

3 המונחים, חלק מהתוכן הרעיוני וציטוטים ערוכים מובאים מדוח ביקורת שנתי 62 לשנת 2011 של מבקר המדינה.

4 מתוך תקן ישראלי 1495 חלק 5, "אבטחת מערכות מידע ממוחשבות - היערכות למצב אסון".

א. הביטוי "אבטחה לוגית" כולל הפעלת מנגנוני תוכנה ייעודיים שנועדה לאפשר גישה מבוקרת למערכות המידע וכן לאפשר בקרה על פעילות המשתמשים.

ב. האבטחה הלוגית מיושמת בדרכים שונות ובעיקר במערכות הפעלה, יישומים, מסדי נתונים, תוכנות ייעודיות ועוד. פעולות האבטחה בתחום האבטחה הלוגית, כוללות, בין היתר: ניהול הרשאות, זיהוי משתמשים, הצפנה, חתימה דיגיטלית, ממשקים נכונים ואבטחתם, שם משתמש, סיסמה וביומטריה להפעלת מחשב ותוכנה או כניסה לבסיס נתונים וניהולם, גילוי ומניעת גישה לא מורשית, ניתוח תנועות הנרשמות ביומני הפעילות – Logs, אמצעי בקרה לגישה מרחוק, אנטי וירוס, Firewall, מבחני חדירה לרשתות הארגון, תחזוקת המערכות ועוד.

16.3. גיבוי ושחזור

במסגרת אבטחת המידע יש לנקוט אמצעים לגיבוי המידע ולשחזורו, להתאוששות מאסון -DRP Disaster Recovery Planning ולהמשכיות עסקית BCP- Business Continuity Plan.

16.4. אבטחת מידע באמצעים ניידים

על אבטחת המידע לכלול גם את המחשבים והאמצעים האחרים הרלוונטיים המנותקים בקביעות או מעת לעת מרשתות הארגון – כגון טלפונים, מחשבים ניידים מחשבי כף יד וכדו'.

הצורך באבטחת המידע ושמירת הפרטיות במועצה האזורית לכיש

17. המועצה האזורית לכיש, ככל רשות מקומית, מספקת שירותים במגוון תחומים המשפיעים על חיי התושבים, וככל גוף ציבורי, היא עושה שימוש הולך וגובר בטכנולוגיה, באתר האינטרנט שלה ובאינטראקציה מקוונת כגון תשלומים, העברת מידע וקבלת מידע.
18. במועצה מידע אישי רב על התושבים, מידע הנוגע לעבודה השוטפת שלה ומערכות מחשוב ורשת מסועפות עם קשרים מחוץ למועצה.
19. הצורך בהגנה על מרחב הסייבר הולך וגדל באופן כללי ובמיוחד עם הגידול בתלות המועצה במערכות הממוחשבות שלה.
20. כאמור לעיל, קיימת מגמת עלייה הן במספר אירועי תקיפות הסייבר והן במורכבותם ותחכומם. פגיעה במרחב הסייבר עלולה להסב נזקים כבדים למועצה, לצנעת הפרט, למסחר, לתקינות וליעילות התפקודית, הארגונית והניהולית.
21. המועצה הולכת ונחשפת למגוון סיכונים בתחום הפרטיות, באבטחת המידע ובאיומי סייבר, שהתממשותם עלולה לגרום נזקים מגוונים הן לעבודת המועצה, הן לתשתיות טכנולוגיות ופיזיות, פגיעה בשירות, ופגיעה בתושבים ובפרטיותם.
22. לאור דברים אלו, מלבד הוראות הדין המחייבות את המועצה, הרי שהמידע המצטבר בידי המועצה, התלות של המועצה במערכות הממוחשבות והסיכונים הקיימים, מחייבים את המועצה לנקוט פעולות לשמירה על המידע שנאסף בידיה ולאבטחתו ולנהל את המידע בצורה מושכלת.

פרק ב' - על הפרטיות ואבטחת המידע - המישור הנורמטיבי

כללי

23. הזכות לפרטיות וחובת השמירה על צנעת הפרט שהוכרו בפסיקה עוגנו בחוק יסוד: כבוד האדם וחירותו, כזכות חוקתית בסעיף 7(א) הקובע, כי: "**כל אדם זכאי לפרטיות ולצנעת חייו**" ובחוק הגנת הפרטיות התשמ"א-1981 (להלן - חוק הגנת הפרטיות), והתקנות שהותקנו מכוחו.

24. חוק הגנת הפרטיות חל הן על המגזר הציבורי והן על המגזר הפרטי, וקובע כי פגיעה בפרטיות תהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית. להלן סקירה קצרה של הוראות חוק הגנת הפרטיות.

25. סעיף 1 לחוק הגנת הפרטיות קובע:

לא יפגע אדם בפרטיות של זולתו ללא הסכמתו.

דרישת ההסכמה בסעיף זה הינה אחד מהעקרונות המרכזיים של החוק. הגדרת "הסכמה" לא קיימת, אלא שהסכמה צריכה להיות מדעת, ולהינתן במפורש או במכללא. באופן עקרוני, איסוף מידע על אדם יוכל להתבצע באם הוא מודע שמידע נאסף אודותיו, הוא מסכים לאיסוף המידע ולשימושים השונים שאוסף המידע מבקש לעשות במידע.

26. בסעיף 2 לחוק הגנת הפרטיות מפורטים המקרים המרכזיים בהם קיימת פגיעה בפרטיות.

(1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;

(2) האזנה האסורה על פי חוק;

(3) צילום אדם כשהוא ברשות היחיד;

(4) פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;

(4א) פרסום תצלומו של נפגע ברבים שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביאו במבוכה, למעט פרסום תצלום בלא השהיות בין רגע הצילום לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות; לעניין זה, "נפגע" – מי שסבל מפגיעה גופנית או נפשית עקב אירוע פתאומי ושפגיעתו ניכרת לעין;

(5) העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו; לענין זה, "כתב" – לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;

(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם ריווח;

(7) הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם;

(8) הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;

(9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;

(10) פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1)

עד

(7) או (9);

(11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד.

27. סעיף 4 לחוק הגנת הפרטיות קובע כי פגיעה בפרטיות היא עוולה אזרחית וסעיף 5 לחוק קובע את הדרכים בהן הפוגע במזיד בפרטיות זולתו מהוות עבירה פלילית.

28. פרק ב' בחוק הגנת הפרטיות עוסק ב"הגנת על הפרטיות במאגרי מידע"; במסגרת זו, סעיף 7 לחוק מציג את ההגדרות הרלוונטיות לנושא, כדלקמן:

"אבטחת מידע" - הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;

"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;

"מאגר מידע" – מרכז להחסנת מידע באמצעות מערכת עיבוד נתונים אוטומטית 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;

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

"מידע רגיש" –

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

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

"רשם" - מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, והממשלה מינתה אותו, בהודעה ברשומות, לנהל את פנקס מאגרי מידע (להלן - הפנקס) כאמור בסעיף 12;

"שלמות מידע" - זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

29. הוראות חוק הגנת הפרטיות בעניין מאגרי המידע, עוסקות בעיקר בעניינים הבאים: רישום מאגר מידע והשימוש בו, בקשה לרישום, סמכויות הרשם, דו"ח הגנה על הפרטיות, חובת מבקש מידע, פנקס מאגרי מידע, זכות עיון במידע, עיון במידע שאינו בהחזקת בעל המאגר, תיקון מידע, תובענה לבית המשפט, סודיות, אחריות לאבטחת מידע, מחזיק במאגרים של בעלים שונים, ממונה על אבטחה, דיוור ישיר.

30. פרק ג בחוק הגנת הפרטיות עוסק בהגנות. סעיף 18 לחוק קובע, כי

במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, תשכ"ה-1965;

(2) הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה:

(א) הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב) הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה;

(ג) הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;

(ד) הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה) הפגיעה היתה בדרך של צילום, או בדרך של פרסום תצלום, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו) הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, תשכ"ה-1965;

(3) בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין, ובלבד שאם היתה הפגיעה בדרך של פרסום - הפרסום לא היה כוזב.

31. סעיפים אחרים בפרק ג עוסקים בפטור, נטל ההוכחה, הפרכה של טענות הגנה ובהקלות.

32. פרק ד לחוק הגנת הפרטיות עוסק במסירת מידע או ידיעות מאת גופים ציבוריים.

33. בהתאם לסעיף 23, "גוף ציבורי" בפרק ד לחוק הינם –

(1) משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;

(2) גוף ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, ובלבד שבצו ייקבעו סוגי המידע והידיעות שהגוף יהיה רשאי למסור ולקבל;

סעיף 23א לחוק הגנת הפרטיות קובע כי הוראות פרק זה יחולו על ידיעות על עניניו הפרטיים של אדם, אף שאינן בגדר "מידע", כשם שהן חלות על "מידע".

סעיף 23ב קובע את איסור מסירת המידע:

(א) מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה.

(ב) אין בהוראות סעיף זה כדי למנוע מרשות בטחון כמשמעותה בסעיף 19 לקבל או למסור מידע לשם מילוי תפקידה, ובלבד שהמסירה או הקבלה לא נאסרה בחיקוק.

34. שאר הסעיפים בפרק ד קובעים את הסייג לאיסור, חובותיו של הגוף הציבורי, הוראות לגבי מידע עודף, הבהרה כי מסירה מותרת אינה פגיעה בפרטיות והוראה בעניין התקנת תקנות.

35. פרק ה לחוק הגנת הפרטיות עוסק בהוראות שונות וביניהן: דין המדינה, מות הנפגע, התיישנות, החלת הוראות מחוק איסור לשון הרע, ראיות על שם רע, אופי או עבר של אדם, צווים שרשאי בית המשפט לצוות בנוסף לכל עונש וסעד אחר, פיצוי בלא הוכחת נזק, אחריות בשל פרסום בעתון, אחריות של מדפיס ומפיץ, עונשין בעבירות של אחריות קפידה, עוולה בנזיקין, חומר פסול לראיה, שמירת דינים, ביצוע, תקנות ואגרות.

36. בקיצור ולענייננו, חוק הגנת הפרטיות כולל מספר עקרונות מרכזיים. אחד מהם הוא עיקרון ההסכמה, המבטא את שליטתו של הפרט על המידע הנוגע אליו – הוא זה שמחליט איזה מידע ייחשף, ולמי. עיקרון זה בא לידי ביטוי, בין היתר, בסעיף 1 לחוק הגנת הפרטיות, הקובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". לפי חוק הגנת הפרטיות, הסכמה בהקשר זה צריכה להיות "מדעת", קרי כזו הניתנת רק לאחר שאדם מבין את משמעות הסכמתו ואת השלכותיה. עיקרון מרכזי נוסף הוא עיקרון צמידות המטרה. לפי עיקרון זה, המוסדר תחת סעיפים 2) 9 (ו-8) ב) לחוק הגנת הפרטיות, מותר להשתמש במידע אך ורק בהתאם למטרה שלשמה הוא נאסף מלכתחילה. שימוש במידע למטרה אחרת מהווה פגיעה בפרטיות. חוק הגנת הפרטיות, והתקנות שהותקנו מכוחו, קובעים גם חובות שונות הנוגעות לרישום מאגרי מידע ולאופן אבטחתם. בין היתר, קיימת חובה לבחון את הצורך בהמשך שמירתו של מידע, בהתאם לתכלית איסופו.

37. חוק הגנת הפרטיות מתייחס גם לזכויות נושא המידע. לפי סעיף 11 לחוק, יש להודיע לנושא המידע (Data Subject) על הכוונה לאיסוף המידע, ולפרט בפניו מהן מטרות השימוש בו והאם מוטלת עליו חובה חוקית למסירתו - או שמותר לו לסרב. סעיף 13 לחוק מעניק לנושא המידע זכות לעיין במידע הנוגע אליו, וסעיף 14 מקנה לו את הזכות לדרוש את תיקונו בנסיבות המתאימות.

38. **הזכות לפרטיות אינה מוחלטת** - להגנה על מידע עשויות להיות תכליות שונות – למשל, מניעת פגיעה במוניטין, מניעת דלף מידע מסחרי, או מניעת דלף מידע פרטי. בעוד שבעיני גורמי המחשוב ההגנה היא לעתים זהה (כגון הצפנה של קובץ או הגדרת עקרונות מחמירים לבקרת גישה), הרי שהתכלית עשויה להיות שונה.

39. כאמור, הזכות לפרטיות הוכרה בחוק יסוד: כבוד האדם וחירותו, בחוקים שונים (ובראשם חוק הגנת הפרטיות) וכן גם באמנות בין-לאומיות. עם זאת, ככל הזכויות, גם הזכות לפרטיות אינה מוחלטת - וייתכנו נסיבות שבהן אינטרסים אחרים יצדיקו פגיעה מסוימת בה. תפיסה זו מוסדרת, בין היתר, בהגנות הקבועות בסעיף 18 לחוק הגנת הפרטיות. עם זאת, פגיעה שכזו צריכה להתבצע בהתאם לתכלית הוראות הדין ולעמוד בעקרונות הכלליים של פעולה בסבירות ותום לב - וכשמדובר בגופים ציבוריים, גם בדרישת המידתיות. ככלל, הגנת סייבר היא פעולה לגיטימית שאין בה כל פגיעה חריגה

בפרטיות. עם זאת, המימוש שלה בפועל צריך להתבצע תוך התייחסות מעמיקה להיבטי פרטיות ועמידה בעקרונות מקובלים, דוגמת:

- עיצוב לאבטחה (Security By Design)
- עיצוב לפרטיות (Design by Privacy)
- הגנה מודעת-איומי (Threat Defense Informed)

עקרונות אלו מחייבים הבנה טכנולוגית-תהליכית מעמיקה מצד ה- CISO ועליו גם לדעת לבצע איזון נכון בין אינטרסים שונים, כך שהמלצותיו להנהלת הארגון יאפשרו קבלת החלטות באופן מושכל[5].

40. כבר כאן ייאמר, כי אבטחת מידע הינה חלק מחובת הרשות המקומית להגנת הפרטיות וצנעת הפרט. היות שמאגרי המידע מכילים פרטים אישיים, ומסירת נתונים על אדם לזולת עלולה לפגוע בפרטיותו, יש לאבטח את המידע. ניתן לקבוע באופן כללי, כי ככל שהפרט עלול להיפגע יותר מחשיפת המידע עליו, כן עולה רמת רגישות המידע וגוברת אחריות הרשות המקומית ורמת האבטחה שעליה לנקוט על מנת להגן עליו.

41. יצוין, כי ככל שחולף הזמן, הרשויות המקומיות עושות שימוש גובר והולך בטכנולוגיה ובמידע, כך בשנים האחרונות גדל מספר "הערים החכמות" העושות שימוש בטכנולוגיות מידע ותקשורת לשיפור הניהול ואיכות החיים של התושבים. מגמה זו מביאה לגידול חד בכמות הנתונים שבידי הרשויות המקומיות, במספר מאגרי המידע שבבעלותן ובתוכן המאגרים הקיימים. פגיעה במערכות המחשוב, במאגרי המידע ובנתונים של הרשויות המקומיות, עלולה להסב נזקים כבדים, ובכלל זה לפגיעה בשירותים הניתנים לתושבים ובצנעת הפרט, ולאור זאת מוטלת עליהן החובה להגן על המידע[6].

42. **תקנות מכח חוק הגנת הפרטיות:**

פירוט התקנות בנושא:

א. תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א – 1981.

ב. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986.

ג. תקנות הגנת הפרטיות (קביעת מאגרי מידע הכוללים מידע שלא לגילוי), התשמ"ז-1987

ד. תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001

ה. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: "תקנות אבטחת מידע").

43. פרק ב לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986 קובע הוראות כלליות לניהול מאגר מידע ופרק ג לתקנות קובע נהלי ביצוע העברת מידע בין גופים ציבוריים ובין היתר הוראות לעניין: ועדה להעברת מידע, אבטחת מידע בעת מסירה,

---

5 קרדיט ל"תורת ההגנה לסייבר בארגון" – מערך הסייבר הלאומי. כאן מופיע רק מידע מנספח ו' למסמך המלא בנוגע לזכות לפרטיות. המסמך עצמו מכיל מידע מקצועי, אשר יישומו בארגון מצריך היכרות עם מערכותיו והתאמה למאפייניו בידי איש מקצוע בתחום הגנת הסייבר. המסמך המלא: https://www.gov.il/he/Departments/General/cyber_security_methodology_2

6 דוח המבקר – 2017.

נוהל מסירה, טיפול במידע עודף, בקשה להעברת מידע. פרק ד עוסק בסדרי ניהול מאגר המכיל מידע מוגבל וכללי השימוש בו.

44. **תקנות אבטחת מידע** – המצורפות כ**נספח ב'** ויידונו להלן – שהותקנו בשנת 2017 מפרטות את אופן יישום חובת אבטחת המידע שנקבעה בחוק הגנת הפרטיות על בעל מאגר מידע אישי, מנהל ומחזיק מאגר. התקנות כוללות מיון של מאגרי מידע לפי מאפיינים שונים וקובעות לפי המאפיינים את רמת האבטחה שחלה על מאגר המידע.

45. התקנות עוסקות בעיקר בנושאים הבאים – בהתאם לסעיפים ולכותרותיהם:

סעיף 1	הגדרות
סעיף 2	מסמך הגדרות המאגר
סעיף 3	ממונה על אבטחת מידע
סעיף 4	נוהל אבטחה
סעיף 5	מיפוי מערכות המאגר וביצוע סקר סיכונים
סעיף 6	אבטחה פיזית וסביבתית
סעיף 7	אבטחת מידע בניהול כוח אדם
סעיף 8	ניהול הרשאות גישה
סעיף 9	זיהוי ואימות
סעיף 10	בקרה ותיעוד גישה
סעיף 11	תיעוד של אירועי אבטחה
סעיף 12	התקנים ניידים
סעיף 13	ניהול מאובטח ומעודכן של מערכות המאגר
סעיף 14	אבטחת תקשורת
סעיף 15	מיקור חוץ
סעיף 16	ביקורות תקופתיות
סעיף 17	שמירת נתוני אבטחה
סעיף 18	גיבוי ושחזור של נתוני אבטחה
סעיף 19	חובות בעל מאגר חלות על מנהל מאגר ומחזיק בו ותיעוד ביצוע פעולה
סעיף 20	סמכויות הרשם

סעיף 21	תחולה וסייגים לתחולה
סעיף 22	תחילה
סעיף 23	הוראת מעבר
סעיף 24	ביטול
סעיף 25	יחס לחיקוקים אחרים
	תוספת ראשונה - מאגרי מידע שחלה עליהם רמת האבטחה הבינונית
	תוספת שנייה - מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה

46. בנוסף לתקנות, הרשות להגנת הפרטיות7 מפרסמת הנחיות בנושא הגנת הפרטיות[8].

47. מאחר שהמועצה היא גוף ציבורי, על רוב מאגריה חלה רמת אבטחה בינונית. יש מאגרים עם רמת אבטחה גבוהה.

48. **דוחות מבקר המדינה** - בחודשים אוקטובר 2016 - ינואר 2017 ערך מבקר המדינה ביקורת בנושא אבטחת המידע והגנת הפרטיות ברשויות המקומיות[9]. הביקורת כללה מעקב אחר אופן תיקון הליקויים שהועלו בביקורת הקודמת בפעולותיהם של 2 עיריות, רמו"ט (כיום הרשות להגנת הפרטיות) ומשרד הפנים בנושא האמור. כמו כן, נבדקו פעולותיהן בנושא של חמש רשויות מקומיות: 3 עיריות, מועצה מקומית ומועצה אזורית. בדיקות השלמה נעשו ברשות הלאומית להגנת הסייבר ובמשרד ראש הממשלה. קטעים מתוך תמצית הדוח מפורטים **<u>בנספח ג'</u>** לדוח זה. דוח נוסף של מבקר המדינה נערך בחודשים יולי-נובמבר 2021 ופורסם ב04/07/2022 ועסק בנושא[10]. בדיקת מבקר המדינה נעשתה בשמונה רשויות מקומיות שנבחרו, תוך מתן ביטוי למחוזות המינהליים שבהם שוכנות הרשויות; למעמדן המוניציפלי; למדד הפריפריאליות שאליו הן משויכות; למדד החברתי-כלכלי שאליו הן משויכות; למגזר שאליו רוב תושביהן משתייכים; ולמספר התושבים המתגוררים בתחום שיפוטן. בדיקות השלמה נעשו במשרד הפנים - במינהל שירותי חירום ובמפעם עמק יזרעאל, במרכז השלטון המקומי ובמערך הסייבר הלאומי שבמשרד ראש הממשלה. כמו כן במסגרת הבדיקה נשלחו

7 בהתאם להגדרת הרשות הפרטיות באתרה: "הרשות להגנת הפרטיות הינה רשם מאגרי המידע הגוף המהווה את הגוף המסדיר, המפקח והאוכף על פי הוראות פרק ב' לחוק הגנת הפרטיות התשמ"א – 1981 על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי. במסגרת תפקידה של הרשות כרגולטור של הזכות להגנת הפרטיות ולהגנת מידע אישי בישראל, הרשות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים מכוח חוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. הרשות פועלת להשגת מטרה זו באמצעות התווית מדיניות, אסדרה, הדרכות, אכיפה מנהלית, אכיפה פלילית ופיקוחי רוחב (Audit). הרשות היא שמתווה את מדיניות ההגנה על המידע האישי במאגרי מידע דיגיטליים. משימותיה המרכזיות של הרשות הן קידום שליטת הפרט במידע אישי על אודותיו, השפעה על תהליכי עיצוב לפרטיות בארגונים ובמערכות מידע בכל מגזרי המשק וחיזוק תחושת המוגנות של הציבור. כל זאת, במטרה לצמצם את הסיכונים הגוברים לפגיעה בפרטיות בעת שמירת מידע דיגיטלי, בעיבודו ובניהולו, והכל תוך איזון ומתן משקל ראוי לחידושים הטכנולוגים וליתרונותיהם עבור השוק והמשתמשים. הרשות להגנת הפרטיות, רואה כמשימתה העיקרית קידום של ציות לדיני הגנת המידע בכל ארגון, עסק וגוף פרטי או ציבורי המנהלים מידע אישי, כך שיפעלו לניהול המידע שברשותם באופן תקין בהתאם לדיני הגנת הפרטיות". חלק מהמתואר בדוח זה, במישור הנורמטיבי\ מבוסס על אתר הרשות.

8 הנחיות אלה מפורטות באתר הרשות להגנת הפרטיות: https://www.gov.il/he/departments/the_privacy_protection_authority/govil-landing-page

9 דוח מבקר המדינה לשנת 2017 "אבטחת מידע והגנת הפרטיות ברשויות המקומיות" - דוחות על הביקורת בשלטון המקומי 2017 (להלן: "דוח המבקר – 2017"). בדוח זה נעשה שימוש בדוח המבקר וחלק מתיאור הדברים והמישור הנורמטיבי מתבסס עליו.

10 דוח מבקר המדינה לשנת 2022 "ניהול מערכות מידע ברשויות המקומיות" - דוחות על הביקורת בשלטון המקומי 2022 (להלן: "דוח המבקר – 2022"). בדוח זה נעשה שימוש גם בדוח המבקר וחלק מתיאור הדברים והמישור הנורמטיבי מתבססים עליו.

שאלונים ל-63 רשויות מקומיות, ו-61 (97%) מהרשויות שנדגמו השיבו עליהם. קטעים מתוך תמצית הדוח מפורטים בנספח ד' לדוח זה.

49. **התחום המקצועי** – בתחום המקצועי ניתן להסתייע בגופים ואנשי מקצוע, בתקנים, המלצות, הנחיות ועוד. מערך הסייבר הלאומי מפרסם חומרים ומסייע לאבטחת המידע, וקיימים נהלים מתקדמים למשרדי הממשלה שניתן ללמוד מהם רבות.

50. מערך הסייבר הלאומי הינו גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום. המערך פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הארגונים והאזרחים, לטיפול בתקיפות סייבר וסילוקן ולהיערכות לחירום. כחלק מתפקידיו, מקדם המערך פתרונות חדשניים וטכנולוגיות צופות פני עתיד, מתווה אסטרטגיה ומדיניות בזירות הלאומית והבין-לאומית, ומפתח את ההון האנושי בתחום. המערך חותר לקיום מרחב סייבר מוגן, בטוח וחופשי עבור כלל האזרחים, המאפשר את צמיחתה ואת ביסוס עוצמתה של מדינת ישראל. המערך פועל מתוקף החלטות הממשלה והחוק להסדרת הביטחון בגופים ציבורים[11].

51. החלטות הממשלה 3611[12], 2443[13], 2444[14] ו-3270[15] עוסקות בהקמת מטה הסייבר הלאומי במשרד ראש הממשלה, בקידום אסדרה לאומית והובלה ממשלתית בתחום הגנת הסייבר, בקידום ההיערכות הלאומית בתחום הגנת הסייבר, בין היתר באמצעות הקמת רשות לאומית להגנת הסייבר במשרד ראש הממשלה ואיחוד מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר ליחידת סמך אחת, שכאמור היא "מערך הסייבר הלאומי".

52. תרשים בעיבוד משרד מבקר המדינה מדוח המבקר - 2022:
חקיקה רלוונטית על ציר הזמן בתחום מערכות מידע 1981 – 2018.

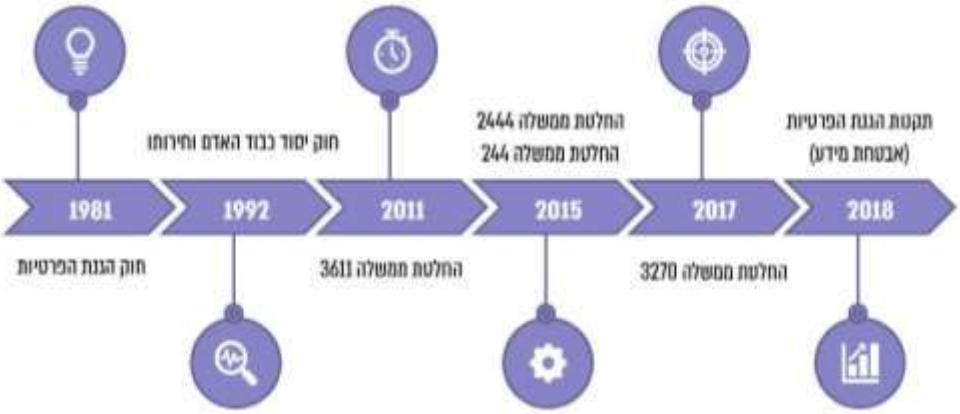
11 מאתר מערך הסייבר הלאומי: https://www.gov.il/he/departments/about/newabout שם כאמור ניתן למצוא חומר מקצועי.

12 החלטת הממשלה 3611 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11).

13 החלטת הממשלה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

14 החלטת הממשלה 2444 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).

15 החלטת הממשלה 3270 "(1) איחוד יחידות מערך הסייבר הלאומי; (2) מתן פטור ממכרז למשרת ראש מערך הסייבר הלאומי; (3) הוספת משרת ראש מערך הסייבר הלאומי לתוספת לפי סעיף 23 לחוק שירות המדינה (מינויים); (4) קביעת שכר ותנאי שירות של ראש מערך הסייבר הלאומי" (17.12.17).



53. מטרת תורת ההגנה הנזכרת לעיל[16], היא להציג בפני המשק הישראלי שיטה מקצועית סדורה לניהול סיכוני הסייבר בארגון. באמצעות המתודה המובאת במסמך תורת ההגנה, הארגון יכיר את הסיכונים הרלוונטיים אליו, יגבש מענה הגנתי ויממש תוכנית להפחתת הסיכונים בהתאם. מרחב הסייבר הוא תולדה של קדמה טכנולוגית, קישוריות וחיבור גלובלי לאינטרנט. התלות הגוברת במרחב הסייבר מביאה עמה בשורות של חדשנות טכנולוגית ופיתוחים אדירים לאדם ולסביבתו. אך לצד אלה מתפתח מרחב איומים, המשפיע על הרציפות התפקודית הארגונית, על שלמות תהליכי הייצור ועל סודיות המידע הארגוני. מתקפות סייבר עלולות לפגוע בארגונים ואף להביא להפסקת תהליכי ייצור ,לנזק כלכלי ולפגיעה במוניטין. מדינת ישראל עושה מאמץ לאומי בהגנת הסייבר במרחב האזרחי. תורת ההגנה הארגונית היא נדבך בתפיסת ההגנה הלאומית, המורכבת מרבדים שונים של הגנה על המשק הישראלי ועל הרציפות התפקודית שלו. תורת ההגנה הארגונית רואה את הארגון כמכלול שלם ומאפשרת את העלאת רמת החוסן הארגוני באמצעות הטמעה רציפה של תהליכים, שיטות ומוצרי הגנה. יישום תורת ההגנה הארגונית ישפר את החוסן הארגוני ואת יכולת העמידה שלו בפני מתקפות סייבר. מרחב סייבר זמין, נגיש ומהימן מהווה תנאי הכרחי להתנהלות בחיי היומיום – ובפרט כשמדובר בעסקים. קל להבין זאת כאשר אלו נמנעים מאיתנו בצורה זמנית. איך ננהל את העסק ללא טלפון סלולרי? ללא הידע האגור ברשת הארגונית? ללא יכולת לבצע סליקת כרטיסי אשראי? במרחב הסייבר יש אפשרויות והזדמנויות מצד אחד, ואיומים וסיכונים מנגד. במרחב זה מתנהלת פעילות ענפה של ריגול מדינתי, ריגול תעשייתי, פשע מאורגן ופשע מזדמן. כל אלה עלולים להשפיע על הביטחון הלאומי (למשל באמצעות פגיעה במרחב הסייבר בתשתית לאומית קריטית כמערכת החשמל או המים) או על התנהלות עסקית (למשל, באמצעות ריגול מסחרי או סחיטה כלכלית). כיום, ארגונים שונים מגינים על עצמם מפני איומים אלו בצורות שונות. באינטרנט קיים מידע רב לגבי דרכי ההתגוננות מפני סיכוני סייבר, והוא מורכב מאוסף של מתודולוגיות סדורות, שיטות עבודה מומלצות, כללי "עשה ואל תעשה" ועוד. ארגונים רבים בארץ ובעולם מתחבטים בשאלות כגון "האם אנחנו משקיעים די בהגנה בסייבר?", "האם אנחנו משקיעים נכון בהגנה בסייבר?" או "האם אנחנו משקיעים בהגנה בסייבר בהתאם למקובל במשק או בענף שלנו?" תורת ההגנה מסייעת לארגונים

16 הקרדיט לדברים המובאים כאן הוא למערך הסייבר הלאומי. כאן מופיעים רק המבואות למסמך וקטעים לשם הפניה אליו. המסמך המלא:
https://www.gov.il/he/Departments/General/cyber_security_methodology_2

למפות את סיכוני הסייבר, להבין את המשמעות הארגונית של התממשות הסיכונים ולהגדיר אמצעי הגנה מידתיים להפחתת הסיכונים העיקריים. תורת ההגנה מלווה בעזרים שונים, שיסייעו לארגון לאמץ אותה בקלות. הם כוללים מסמכי הרחבה מקצועית, נוהלי הגנה והמלצות ליישום עבור תחומים שונים, טבלאות ישימות מול חקיקה ורגולציה ישראלית ותקינה בינלאומית, מיכון התורה באמצעות פלטפורמה טכנולוגית נוחה – ועוד.

54. העיקרון הראשי של תורת ההגנה הוא הגנה מפני איומים רלוונטיים – כלומר, ההכרה בכך שכאשר באים להגן על רציפות התפקוד של הארגון, נכסיו ויעדיו יש להתבסס על הבנת איום הייחוס, המודיעין והמגמות המשתנות בתחום הרלוונטי.

55. עקרון זה, בא לידי ביטוי באמצעות תתי העקרונות הבאים:

א. אחריות ההנהלה האחריות להגנה על המידע נמצאת בראש ובראשונה אצל הנהלת הארגון.

ב. הגנה מתוך ראיית היריב. המשקל של המלצות ההגנה, כמו גם התפיסה המובאת להגדרת סדר העדיפויות למימושן, נגזר ישירות מתוך הבנת תרחישי התקיפה הנפוצים ומידת היעילות של המלצות ההגנה אל מול תרחישים אלו .המלצות ההגנה הינן האמצעי להשגת התכלית של רמת חוסן ארגונית בהתאם לאיומים ודרכי פעולת תוקף הרלוונטיים לארגון.

ג. הגנה מבוססת ידע וניסיון ישראלי. תורת ההגנה מאפשרת את המיקוד בסיכונים הרלוונטיים לכל ארגון וארגון. כחלק מפעילות מערך הסייבר הלאומי, מתבצעות ביקורות והערכות מודיעין עתיות למשק. פעולות אלו מאפשרות למקד ארגונים באזורים ספציפיים במעגלי ההגנה השונים.

ד. הגנה בהתאם לפוטנציאל הנזק ההשקעה בהגנה על כל יעד הגנה תהיה בהתאם לרמת הקריטיות שלו לתפקוד הארגון.

ה. הגנה מבוססת עומק יישום. בקרות תורת ההגנה, מאפשרות לארגון ליישמן ברמות שונות של בשלות. מעבר מהסתכלות על הבקרות מתוך נקודת מבט של "ציות" (Compliance)בנושאים כגון DLP, SOC סקרי סיכונים ועוד לנקודת מבט של אפקטיביות ההטמעה שלהן. הדבר בא לידי ביטוי באמצעות הגדרת "עומק יישום" לכל המלצת הגנה (בקרה) והגדרת "ראיות נדרשות" בהתאם.

56. **מערכת יוב"ל** - במהלך ביצוע בדיקות הביקורת, עלו שאלות מעובדים בדבר היכולת לבחון את רמת הגנת הסייבר במועצה. אחד הכלים הוא מערכת יוב"ל ש"היא פיתוח של מערך הסייבר הלאומי שנועד לאפשר לכל ארגון בישראל לבדוק את רמת הגנת הסייבר שלו. זהו מחשבון סייבר ייחודי המאפשר בדיקה מקיפה לגבי עמידה בתקנים מקומיים ובין-לאומיים בצורה אנונימית, דינמית ופשוטה. המערכת מנגישה לארגונים קטנים, בינוניים וגדולים במשק וללא עלות כלים מתקדמים לניהול סיכוני סייבר.

57. המערכת בנויה בצורת סידרה של שאלות שנועדו לקבוע את רמת ההגנה הנוכחית בנושאים של הגנת מידע, רשתות, גיבויים, פיתוח מאובטח ועוד. באמצעות הזנת פרמטרים פשוטים למערכת, יכול נציג הארגון לקבל תמונת מצב רחבה על מצב הגנת הסייבר בארגון שלו ולנהל סיכונים בהתאם. התשובות המתקבלות מהזנת הפרמטרים עונות על הצורך של הארגון באבטחה ובניהול סיכונים, על מידת ההלימה לרגולציות מקומיות ובין-לאומיות וגם על העשייה של מנהלות הגנת הסייבר בארגון. לבסוף,

המערכת יכולה להציג את תעדוף הטיפול הנדרש לפי שלבים ורמות חומרה לארגון. הארגון יכול להפיק דו"ח המציג את תמונת המצב באמצעות המערכת ולגזור בהתאם את תוכנית העבודה.

58. המערכת ייחודית בכך שהיא מנגישה את המתודה הלאומית להגנת סייבר בחינם לכלל המשק. הארגונים מקבלים תובנות ספציפיות לארגונם המסתמכות על תוצרי מערך הסייבר הלאומי ובפרט תורת ההגנה הלאומית של המערך, כך שהנטל בעבודה מול דוחות רבים והמלצות מגוונות להגנה מצטמצמים למקום אחד.

59. ראש מרכז מתודולוגיה ובדיקות חוסן במערך הסייבר לאומי יובל שגב, אשר עמד בראש הפרויקט, הסביר כי "מטרת המערכת להקל על הארגונים בהערכת המצב העכשווית שלהם ולהגיע למצב שבו החזר ההשקעה על הזמן שהוקדש לבחינת רמת ההגנה בארגון הוא הגבוה ביותר. בהשקעה של כמה שעות עד ימים בודדים הארגון מקבל תמונת מצב מקיפה על רמתו. מדובר בתפיסה חדשנית המאפשרת לשנות את רמות ההגנה במשק בזמן אמת".

60. המערכת מפיקה תמונת מצב, שחשופה לעיני הארגון בלבד, על עמידתו בסטנדרטים להגנת סייבר, כפי שנקבעו בתורת ההגנה של המערך, וכן הצעה לביצוע פעולות נדרשות. למחשבון שתי קטגוריות, הראשונה לביצוע סקר סיכונים לעסק קטן אל מול עשרה כללי אצבע פשוטים ובסיסיים ליישום לצורך הגנה. השנייה עבור ארגון בינוני או גדול, המאפשרת למפות את נכסיו והתהליכים העסקיים, לדרג אותם בהתאם לרמת הסיכון ולקבל את רמת התאימות לתקנים, תרחישי תקיפה ותוכנית עבודה מסודרת. המערכת נותנת ציונים במספר משתנים, אשר מונים את הבקרות התקינות מול הלא תקינות ומציגות את רמת ההגנה של הארגון בכל אחת מחמש הפונקציות העיקריות בהגנה: זיהוי, הגנה, איתור, תגובה והתאוששות.

61. המערכת מספקת לארגון יכולת לעקוב אחר התקדמות התהליך ולמקסם את הערך מכל תוצר מתודולוגיה אותו המערך מפתח, על ידי הנגשתו במקום ובזמן המתאים. המטרה מאחורי הקמת מערכת זו היא לתת לעסקים ולארגונים כלי יעיל וחכם ללא עלות וזאת במטרה לסייע למשק להגביר את החוסן ואת רמת ההגנה בתחום הסייבר"[17].

62. יצוין, כי תקנה 20(ב) לתקנות אבטחת המידע קובעת שהרשם רשאי להורות כי מי שיעמוד בהוראות מסמך מנחה בעניין אבטחת מידע או בהנחיות של רשות מוסמכת בעניין אבטחת מידע החלות עליו, יראו אותו כמקיים הוראות התקנות כולן או חלקן, אם השתכנע כי עמידה בהוראות המסמך המנחה בעניין אבטחת מידע או בהנחיות הרשות המוסמכת, לפי העניין, באופן שהורה לפי תקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע; לעניין זה "רשות מוסמכת" –גוף ציבורי המוסמך על פי דין לתת הנחיות בעניין אבטחת מידע;
"מסמך מנחה בעניין אבטחת מידע" – תקן רשמי, תקן ישראלי או תקן בין-לאומי כמשמעותם בחוק התקנים, התשי"ג-1953, או מסמך ייחוס, שהרשם אישר לעניין זה.

63. בהקשר זה, יובהר כי מכון התקנים הישראלי פרסם מספר תקנים, בעלי מעמד שונה, בעניין אבטחת מידע וסייבר, אשר מהווים מכלול תקנים, שניתן לראות בהם נורמה מקיפה לאבטחת מידע בארגונים, לרבות:

מספר תקן	כותר

17 https://www.gov.il/he/departments/general/yuvalinfo האמור לעניין בעניין המערכת – מאתר זה.

ת"י 1080 חלק 8	טכנולוגיית המידע - הגדרות מונחים: אבטחת מידע
ת"י 6000 חלק 3	מערכת גדר התרעה: תקשורת ואבטחת מידע-התקנת דגם ובדיקתו
ת"י 10181 חלק 4	טכנולוגיית המידע-חברור מערכות פתוחות - מסגרות אבטחת מידע למערכות פתוחות: מסגרת אי-התכחשות
ת"י 19772	אבטחת מידע - הצפנה מאומתת
ת"י 27000	טכנולוגיית המידע - טכניקות אבטחה - מערכות לניהול אבטחת מידע - סקירה כללית מונחים והגדרות
ת"י 27001	טכנולוגיית המידע - טכניקות אבטחה - מערכות לניהול אבטחת מידע - דרישות
ת"י 27002	טכנולוגיית המידע: טכניקות אבטחה - קובץ כללים לניהול אבטחת מידע
ת"י 27003	טכנולוגיית המידע - טכניקות אבטחה - מערכות לניהול אבטחת מידע - הנחיות
ת"י 27004	טכנולוגיית המידע - טכניקות אבטחה - ניהול אבטחת מידע - ניטור מדידה ניתוח והערכה
ת"י 27005	טכנולוגיית המידע - טכניקות אבטחה - ניהול סיכוני אבטחת מידע
ת"י 27006	טכנולוגיית המידע - טכניקות אבטחה - דרישות לגופים העורכים מבדקים ומספקים התעדה למערכות לניהול אבטחת מידע
ת"י 27007	טכנולוגיית המידע - טכניקות אבטחה - קווים מנחים לעריכת מבדקים של מערכות לניהול אבטחת מידע
ת"י 27010	טכנולוגיית המידע - טכניקות אבטחה - ניהול אבטחת המידע של תקשורת בין-מגזרית ושל תקשורת בין-ארגונית
ת"י 27011	טכנולוגיית המידע - טכניקות אבטחה - קובץ כללים לבקרות אבטחת מידע המבוססות על התקן הישראלי ת"י (27002 עבור ארגוני בזק (טלקומוניקציה
ת"י 27014	טכנולוגיית המידע - טכניקות אבטחה - ניהול אבטחת מידע
ת"י 27016	טכנולוגיית המידע - טכניקות אבטחה - ניהול אבטחת מידע - כלכלה ארגונית
ת"י 27017	טכנולוגיית המידע- טכניקות אבטחה - קובץ כללים לבקרות אבטחת מידע לשירותי ענן המבוססות על התקן 27002 הישראלי ת "י
ת"י 27019	טכנולוגיית המידע - טכניקות אבטחה - בקרות אבטחה מידע לתעשיית התועלת האנרגטית

ת"י 27035 חלק 1	טכנולוגיית המידע - טכניקות אבטחה - ניהול אירועי אבטחת מידע: עקרונות לניהול ארועים
ת"י 27035 חלק 2	טכנולוגיית המידע - טכניקות אבטחה - ניהול אירועי אבטחת מידע: קווים מנחים לתכנון והכנה עבור תגובה לאירוע
ת"י 27035 חלק 3	:טכנולוגיית המידע - ניהול אירועי אבטחת מידע קווים מנחים לפעולות תגובה לאירועים בטכנולוגיית המידע (ICT).
ת"י 27036 חלק 1	טכנולוגיית המידע - טכניקות אבטחה - אבטחת מידע לקשרי ספקים: סקירה כללית ומושגים
ת"י 27036 חלק 2	טכנולוגיית המידע - טכניקות אבטחה - אבטחת מידע לקשרי ספקים: דרישות
ת"י 27036 חלק 3	טכנולוגיית המידע - טכניקות אבטחה - אבטחת מידע לקשרי ספקים: קווים מנחים לאבטחת שרשרת האספקה בטכנולוגיית המידע והתקשורת
ת"י 27036 חלק 4	טכנולוגיית המידע - טכניקות אבטחה - אבטחת מידע.לקשרי ספקים: קווים מנחים לאבטחה של שירותי ענן
ת"י 27799	אינפורמטיקה בתחום הבריאות - ניהול אבטחת מידע בתחום הבריאות באמצעות שימוש בתקן הישראלי ת"י 27002
ת"י 27034 חלק 5	:טכנולוגיית המידע - טכניקות אבטחה - אבטחת יישומים מבנה נתונים של פרוטוקולים ושל בקרות אבטחת יישומים
ת"י 27034 חלק 6	:טכנולוגיית המידע - טכניקות אבטחה - אבטחת יישומים חקר מקרים
ת"י 27038	טכנולוגיית המידע - טכניקות אבטחה - מפרט להסרה דיגיטלית של מידע
ת"י 6000 חלק 1	2 מערכת גדר התרעה :כללי-רמת אבטחה
ת"י 6021	אבטחת התקשורת והמידע במערכות ממוחשבות מבוססות יחידות קצה
ת"י 9594 חלק 8	:טכנולוגיות המידע - חברור מערכות פתוחות - המדריך מסגרות עבודה של מפתח פומבי ותעודת מאפיינים
ת"י 14971	התקנים רפואיים - יישום ניהול סיכונים להתקנים רפואיים

ת"י 15408 חלק 1	טכנולוגיית המידע - טכניקות אבטחה - קריטריונים להערכת אבטחה לטכנולוגיית המידע: הקדמה ומודל כללי
ת"י 27013	טכנולוגיית המידע - טכניקות אבטחה - הנחיות ליישום משולב של התקנים הישראליים ת"י 27001 ות"י 20000 חלק 1
ת"י 27018	טכנולוגיית המידע - טכניקות אבטחה - קובץ כללים בעננים ציבוריים (PII) להגנה על מידע מזהה אישי הפועלים כמעבדי מידע מזהה אישי
ת"י 27021	טכנולוגיית המידע - טכניקות אבטחה - דרישות כשירות
ת"י 27031	טכנולוגיית המידע - שיטות אבטחה - קווים מנחים למוכנות טכנולוגיות המידע והתקשורת לרציפות עסקית
ת"י 27032	טכנולוגיית המידע - טכניקות אבטחה - קווים מנחים לאבטחת סייבר
ת"י 27033 חלק 1	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת סקירה כללית ומושגים:
ת"י 27033 חלק 4	טכנולוגיית המידע - טכניקות אבטחה - אבטחת רשת אבטחת תקשורת בין רשתות באמצעות שערי אבטחה (GATEWAYS):
ת"י 27040	טכנולוגיית המידע - טכניקות אבטחה - אבטחת אחסון
ת"י 27041	טכנולוגיית המידע - טכניקות אבטחה - הנחיות להבטחת.התאמה והלימות של שיטה לחקירת אירוע
ת"י 27043	טכנולוגיית המידע - טכניקות אבטחה - עקרונות ותהליכים בחקירת אירוע
ת"י 27701	27001 טכניקות אבטחה - הרחבה לתקנים הישראליים ת"י ות"י 27002 עבור ניהול פרטיות המידע - דרישות וקווים מנחים
ת"י 80030	מדריך לביצוע הערכת סיכונים

64. עוד יוזכר כאן, כי המועצה המייעצת לביקורת ואבטחת מידע באגף הבכיר לביקורת המדינה במשרד ראש הממשלה, פרסמה כבר בספטמבר 2005 "נוהל מסגרת לאבטחת מידע" (להלן - נוהל המסגרת), אשר שתי מטרותיו העיקריות: להנחות את המנהל הכללי וגורמי המטה במשרדי הממשלה, להכנת מסמך "מדיניות אבטחת "המידע הרגיש" ומערכי המידע", אשר באחריות המשרד, ולהטמיעו בקרב כל עובדי המשרד; לתאר בפני כל עובדי המשרד המטפלים, עוסקים, או נעזרים ב"מידע רגיש", ובמערכי המידע, השליטה והבקרה, את העקרונות לאבטחת "מידע רגיש" ומערכי מידע, שליטה ובקרה, שנקבעו על ידי המועצה המייעצת לביקורת ואבטחת מידע. אומנם נוהל המסגרת דאז, כבר

ישן ואומנם איננו חל על המועצה, אך הדברים מובאים על מנת להראות שהדברים אינם חדשים. דברים אלו הובאו גם בדוח הקודם בעניין אבטחת המידע.

65. נוהל המסגרת כולל 38 נהלים לאבטחת מידע במשרדי הממשלה:

<u>א. קביעת מדיניות ומיפוי מידע</u>

1. קביעת מדיניות אבטחת "מידע רגיש" ומערכי מידע בממשלה ומוסדותיה
2. מיפוי וסיווג של "מידע רגיש" ומערכי מידע
3. סקרי סיכונים - ניהול והערכה
4. גורמי אבטחת מידע – הגדרות ותפקידים
5. ועדות היגוי למחשוב

<u>ב. הגורם האנושי ואבטחת המידע</u>

6. בדיקת מהימנות העובדים, התחייבות לשמירת הסודיות
7. קשר עם גורמי חוץ ב-outsourcing (מיקור חוץ)
8. מודעות, הדרכה, הטמעה והסברה
9. הנדסה חברתית – Social Engineering
10. ביקורת של אבטחת מידע
11. תוכנית הכשרה של אחראים על אבטחה וביקורת של המידע

<u>ג. אבטחה לוגית</u>

12. בקרת גישה למחשב המרכזי ולמחשבים האישיים
13. מידור, זיהוי והרשאות המשתמשים
14. זיהוי ואימות משתמשים באמצעים ביומטריים
15. בקרה ופיקוח לוגי
16. קבלת מערכת מידע חדשה
17. הטמנות תוכנה / חומרה במערכות מידע ממוחשבות
18. אבטחת פעילות פיתוח ותחזוקה של מערכות מידע

<u>ד. אבטחה פיזית</u>

19. טיפול במסמכי קלט/פלט
20. ניהול ואבטחה של אמצעי אחסון מגנטיים ואופטיים
21. העברת מידע והוצאתו

22. רישום המאגרים
23. ניהול מלאי חומרה ותוכנה
24. אבטחת רשומות ותעודות רשמיות
25. שימור רשומות אלקטרוניות
26. ביעור רשומות
27. סיכוני אש, חשמל ומים בחדר המחשב

ה. גיבוי, שחזור והתאוששות

28. גיבוי ושחזור מידע
29. תוכניות התאוששות מאסון (Disaster Recovery Planning–DRP)

ו. אבטחת מידע במחשבים המנותקים מרשתות המשרד

30. אבטחת תוכנה וחומרה במחשבים אישיים
31. אבטחת מידע במחשבים ניידים, palm pilot ו-דיסקים נתיקים

ז. אבטחת תקשורת ושימושי אינטרנט

32. אבטחת תוכנה ברשתות מקומיות
33. אבטחת התקשורת
34. אבטחת מידע בשימוש באינטרנט
35. תוכנות פוגעניות במחשב אישי וברשת מקומית
36. התקנה ואבטחה של תוכנות השתלטות מרחוק
37. הפעלה ושימוש במודמים
38. שימוש בפקס להעברת "מידע רגיש" או מסווג

פרטיות במועצה האזורית

66. כאמור, הרשות המקומית מספקת שירותים במגוון תחומים בממשק ישיר לחיי התושבים כחינוך, בריאות, רווחה, איכות הסביבה, פיתוח פיסי וחברתי, תרבות וביטחון אישי. במסגרת שירותיה ועבודתה, מצטבר מידע הכולל, בין היתר, נתונים על אישיותו של אדם, מעמדו האישי, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו אמונתו וכן "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות, כגון אבחונים פסיכולוגיים, חוות דעת של פסיכולוגים, עובדים סוציאליים ועוד.
67. מאגרי המידע של הרשות מכילים פרטים אישיים וסודיים רבים, שחשיפתם עלולה לפגוע בפרטיות ולהסב נזקים שונים. פגיעה במערכות הממוחשבות ברשויות המקומיות ובמידע האצור בהן, עלולה להסב נזקים כבדים לצנעת הפרט, לתקינות וליעילות התפקודית, הארגונית והניהולית.
68. במחלקות המועצה מנוהל מידע אישי רגיש, לרבות:

א. מחלקת הרווחה – נתוני מטופלים

ב. מחלקת החינוך – נתוני קטינים

ג. שפ"ח – נתוני קטינים מטופלים

ד. מחלקת הגביה – נתוני תושבים

ה. מחלקת משאבי אנוש

ו. מחלקת שכר

ז. מצלמות אבטחה

ח. המוקד העירוני – הקלטות ותיעוד פניות תושבים

69. **הסיכון לפרטיות ברשויות המקומיות** – "פוטנציאל הסיכון לפרטיות ברשויות המקומיות, גם בהשוואה למגזרים שונים במשק, גבוה במיוחד. הרשויות מנהלות ומחזיקות במידע רחב היקף ורגיש על תושביהן, לרבות מידע ממרשם האוכלוסין הכולל מידע אישי כגון מספרי תעודת זהות, כתובת מגורים, דרכי יצירת קשר, מצב הנכסים ובעליהם לרבות שווי הנכס, קיומה של משכנתא, נתונים על גביה ואכיפתה, מידע אודות תלמידים, מידע על הטיפול בלשכות הרווחה, ואף מידע אודות יעוץ פסיכולוגי וסוציאלי שמקבלים תושבי הרשויות. בנוסף, הרשויות מחזיקות במאגרי מידע רבים מתחומים שונים כגון רווחה, חינוך, דיור ועוד, המאפשרים הצלבה של פרטי מידע, דבר המגביר את החשש לשימוש במידע הקיים לצרכים החורגים ממטרת איסופו המקורית. העובדה כי הרשויות אף נעזרות לעתים קרובות בנותני שירותים חיצוניים, מאפשרת, במצבים מסוימים, חשיפה של גורמים נוספים למידע רגיש הקיים במאגרי הרשות המקומית. יודגש, כי הרשויות המקומיות הן גופים ציבוריים, וככאלה הן מוסרות ומקבלות דרך קבע מידע אישי אודות תושבים מגופים ציבוריים אחרים, כגון רשות האוכלוסין. כמו כן, הן מחזיקות במנגנוני מחשוב גדולים שעשויים לייצר גישה למידע למספר רב של מורשי גישה"[18].

70. **ערים חכמות** - המציאות בימינו דורשת שימוש הולך וגובר בטכנולוגיה, רשויות מעוניינות לפעול ב"ערים חכמות" ודיגיטליות. מציאות זו מהווה אתגר גם בתחום הפרטיות.

71. המידע על תושבים, אורחים, עובדים, עסקים, ארגונים ועוד, נאסף פעמים רבות באופן עקיף וחד-צדדי באמצעים טכנולוגיים ובניטור אוט', מעובד, מנותח ונאסף במאגרי הרשויות.

72. "אם בעבר זליגת מידע אישי ופגיעה בפרטיות היתה יכולה ל"הסתכם" ברכילות, מבוכה או סנקציות חברתיות על הפרט, העיר החכמה משקפת את אתגרי "הדור הבא" של הפרטיות ו"מחירים" חמורים יותר. אנו חיים בעידן שבו הטכנולוגיות מאפשרות מעקב תמידי אחר התושב, שלל שימושים במידע שנאסף, והפקת תובנות נוספות מהמידע. תוצאות המציאות הזו עשויות להיות לטובת התושבים והחברה, אך יתכנו גם היבטים שליליים שיש להביא בחשבון כעודף התערבות מצד העירייה בחיי התושבים, הגברת המישטור שיוביל לצעדי אכיפה וענישה ופגיעה במרקם החיים האינדיבידואלי

18 הרשות להגנת הפרטיות - https://www.gov.il/he/departments/news/news_audit_report_local_municipality

המשגשג דווקא בהיותו בלתי מפוקח ובלתי מנוטר. איסוף מידע באמצעות מצלמות וחיישנים מסוגים שונים משמש ערים חכמות כבר כיום לייעול תהליכי עבודה פנימיים, שיפור השירותים לתושבים וכן שמירה על בטיחותם וביטחונם. היתרונות הרבים הגלומים באיסוף מידע שכזה אינם במחלוקת, עם זאת הם גם מהווים בסיס למנגנוני מעקב ציבורי תמידי, אשר עלולים לפגוע בפרטיות התושבים. בעיר ניו יורק, לדוגמא, נתגלה כי סנסורים חכמים הפזורים בעיר קוראים את כרטיס ה 'Pass-EZ' - של התושבים ללא ידיעתם וכך אוספים מידע לגביי מיקומם של כלי רכב. במקור כרטיס זה אמור לשמש לשם מעבר מהיר במחסומים של כבישי אגרה, כפי שסביר שמרבית המשתמשים בו הניחו, אולם בו בזמן התברר כי נאסף מידע אודות מיקום המשתמשים, דבר העלול לפגוע בפרטיותם. הקו הדק שבין ניטור התנהגות לבין הרצון להכתיב אותה הולך ומיטשטש. ערים חכמות עוסקות כבר כיום בהכוונת התנהגות תושבים, בין אם מדובר בשינוי הרגלי צריכת אנרגיה ומים לטובת הגברת הקיימות, שינוי הרגלי חניה, נהיגה ונסיעה לטובת הפחתת עומסי תנועה בעיר או שינוי הדרך שבה תושבי העיר הצעירים לומדים ומתחנכים. יתכן שדוגמאות אלו יביאו להטבה באיכות חייהם ורווחתם של התושבים, אך ללא חשיבה, בקרה והצבת גבולות, יתכנו גם שימושים במידע שייאסף על אנשים אשר לא יהיו לטובתם ויפגעו באינטרסים שלהם. אתגר נוסף שעומד בפני הרשויות המקומיות בהיבט הפרטיות, הוא היעדר אלטרנטיבה. בשוק הפרטי מודל עסקי של חברות רבות מאפשר מתן שירות או מוצר בתמורה למידע שנמסר על ידי המשתמש, וזאת מכיוון שמידע אישי רב על משתמשים מהווה לרוב יתרון תחרותי. בהנחה שהדבר הובא לידיעתם, למשתמשים אלה יש מידה מסוימת של שליטה מתי, איך ועד כמה הם מוותרים על המידע האישי שלהם בתמורה לשירותים. לעומת זאת, ל'משתמשי' העיר החכמה (התושבים) אין אלטרנטיבה לקבלת שירותים ציבוריים והם אינם יכולים להימנע מאיסוף המידע עליהם מבלי ש"ישלמו" על כך, בין היתר, בביטחון ובאיכות החיים, בפרט כאשר מדובר במידע שנאסף בתשתיות עירוניות חיוניות, כמו במערכת רכבות יחידה בעיר, מערכת החשמל ומערכות המים וכו'. בכך עשוי להתערער יסוד ההסכמה של התושב לשימושי הרשות במידע על אודותיו, מאחר שאין לו אפשרות לבחור בחלופה אחרת. על כן, מתחייבת זהירות רבה יותר של הרשות בדרישה לשימוש במידע אישי של תושביה. בנוסף למחסור בכוחות שוק תחרותיים שעשויים לסייע בשמירה על הפרטיות בעיר החכמה, איסוף המידע שמבצעת הרשות המקומית מאתגר גם את עקרון צמידות המטרה. לא תמיד ברור האם השימוש שנעשה במידע הנאסף על-ידי העיריה הוא אכן למטרה שהוגדרה ולה בלבד. ישנן דוגמאות מערים בעולם שבהן מידע שהצטבר בידי השלטון המקומי "נדד" גם לרשויות אחרות (שלטון מרכזי או רשויות אכיפת החוק) ואף לגורמים מסחריים, ושימש למטרות שאינן המטרות אשר לשמן אישר התושב את איסוף המידע עליו או שהעירייה רשאית הייתה לאסוף ולהשתמש בו מתוקף סמכותה על פי דין. לדוגמא, תושב המשתמש בפלטפורמה עירונית המאפשרת לדווח על מפגעים תשתיתיים בעיר באמצעות העלאת תמונות, יתכן שהיה בוחר שלא להעלותן לו היה מודע לשימוש שנעשה במידע, ככל שנעשה, מעבר לשימוש הספציפי במידע שהעביר למטרה שלשמה הועבר .אתגר נוסף לרשויות המקומיות בעת הטמעת עיר חכמה, הוא ריבוי המידע המצטבר במאגריה המגדיל את הצורך של הרשות המקומית להשקיע באבטחת מידע, על מנת למנוע דליפת מידע אישי של התושבים. בנוסף, מאגרי המידע הללו עשויים להוביל לניתוחים מוטים והסקת מסקנות לא נכונות ואף עלולים להביא להקצאת משאבים לא נכונה, לאפליית אוכלוסיות מסוימות ואף לצעדים לא אתיים הפוגעים בחרויות הפרט ובשוויון. טכנולוגיות הניטור השונות והניבוי האנליטי מייצרות אתגרים לפרטיות, אך הן עשויות גם להיות חלק ממסגרת המייצרת ערך רב לתושב ולעירייה, יחסי אמון עם הרשות המקומית והעצמת אוכלוסיות. על אף אתגרי הפרטיות הרבים והמורכבים העומדים

בפני הרשות המקומית והתושבים בערים חכמות, ישנן דרכים רבות למזעור אתגרים אלה ולניהול הסיכונים באופן מושכל המאפשר הגנה על פרטיותם של התושבים".[19]

73. החובות הכלליות בחוק ביחס לאיסוף ולשימוש במידע אישי[20]

<u>ניהול מאגרי מידע - כללי</u>

ברשויות ובמיוחד בערים החכמות, מצטברת כמות עצומה של מידע במאגרים שונים. החל ממאגרים בסיסיים המכילים מידע על תושבי היישובים בתחומים שונים כמו רווחה, חינוך, משאבי אנוש, רישוי עסקים, ארנונה וגבייה. ועד מאגרים הייחודיים לערים החכמות, כמו מאגרי מידע המצטברים מרשת ה WiFi-העירונית, מכרטיסי התושב המקומיים או מאפליקציות שונות שמפעילה הרשות המקומית או העיריה לטובת התושבים, לעיתים קרובות באמצעות גורמים חיצוניים וקבלני משנה. מאגרי מידע אלה, המגיעים ממקורות רבים, מצטלבים בנקודה מסוימת ומחייבים את הרשות או העיריה לנהלם בצורה מאובטחת, תוך הקפדה על דגשי ניהול מאגרי מידע ותקנות אבטחת מידע, על מנת למנוע זליגת מידע אישי של תושבים. למעט מספר חריגים מצומצם, מאגר מידע הוא 'אוסף נתוני מידע על אדם הניתן לזיהוי והמוחזק באמצעים דיגיטליים', כמוגדר בחוק הגנת הפרטיות, תשמ"א-1981.

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

א. **חובת הרישום** – בנסיבות מסוימות, המפורטות בסעיף 8(ג) לחוק, נדרש בעל מאגר מידע לרשום את המאגר אצל הרשות להגנת הפרטיות. מאגר מידע של רשות מקומית בישראל חייב ברישום, שכן מדובר בגוף ציבורי על פי הוראות החוק.

ב. **אין לעשות שימוש במידע שלא למטרה שלשמה נמסר ונאסף** – מחובתה של הרשות המקומית לעמוד בעקרון 'צמידות המטרה', אשר קובע כי **ניתן לעשות שימוש במידע הנאגר אך ורק לטובת המטרה שלשמה הוא נאסף ולא לשם אף מטרה אחרת** - סעיף 8(ב).

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

- **חובת מתן הודעה** – העיריה מחויבת ליידע את הפרט, בטרם איסוף המידע, האם מחובתו החוקית למסור את המידע או לא (למשל, לצורך קביעת גובה מיסי

19 מתוך פרק 3 ב"מדריך הגנת הפרטיות לעיר החכמה" של הרשות להגנת הפרטיות. לגרסה המלאה: https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

20 פרק זה מתוך "מדריך הגנת הפרטיות לעיר החכמה" של הרשות להגנת הפרטיות בקישור הנ"ל.

ארנונה, התושב מחויב למסור מידע רלוונטי), מה המטרה שלשמה נאסף המידע, למי יימסר המידע ומה תהיה מטרת המסירה (לפי סעיף 11 לחוק).

- **זכות עיון במידע** – חובת העיריה לאפשר לכל פרט עליו נאגר מידע, את זכות העיון בנתונים שנאספו עליו, תחת כמה מגבלות (המפורטות בסעיף 13 לחוק).
- **זכות תיקון המידע** – נושא המידע רשאי לדרוש תיקון של מידע אודותיו, ככל שהמידע במאגר אינו נכון)כמפורט בסעיף 14 לחוק).
- **חובת הסודיות** – בעל מאגר המידע, המחזיק בו ומי מעובדיו, מחויבים בשמירת סודיות המידע אליו נחשפו כחלק מעבודתם (סעיף 16 לחוק).

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

ה. חובה נוספת של בעל מאגר המידע והמחזיק בו, היא חובת אבטחת המידע (המפורטת בסעיף 17 לחוק) כן עמידה בתקנות אבטחת מידע.

74. תקנות אבטחת מידע - כללי

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

מחובת כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה. בהתאם להגדרת רמת האבטחה של המאגר תבחן הרשות המקומית אילו תקנות חלות על המאגר. **מאגר שבבעלות גוף ציבורי, כמו רשות מקומית, חלה עליו רמת האבטחה הבינונית, לכל הפחות**. רמת האבטחה הגבוהה תחול על מאגר שבבעלות גוף ציבורי כאשר הוא מכיל מידע אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה לעיון ופעולות בו עולה על 100 מורשים אשר מטרתו העיקרית היא לדיוור ישיר, או כולל מידע הנוגע לצנעת חייו האישיים של אדם; מידע רפואי או מצב נפשי; מידע גנטי; עמדות פוליטיות או אמונות דתיות; עבר פלילי ; נתוני תקשורת; נכסים והתחייבויות כלכליות והרגלי צריכה של אדם אשר יש בהם ללמד על מידע כאמור.

בהתאם לרמת האבטחה הנדרשת למאגר המידע, להלן טבלת הסבר[21] המפרטת אילו תקנות חלות על המאגר.

21 מתוך המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע): https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf תיאור המישור הנורמטיבי מובא גם ממדריך זה.

להלן מובאות בתמצות התקנות הרלוונטיות והסבר המפרט אילו תקנות חלות על המאגר למאגרים עליהם חלות רמות האבטחה הבינונית והגבוהה:

א. **חובת הרשות המקומית לנהל 'מסמך הגדרות מאגר', לכל מאגר בכל רמת אבטחה**, וזאת בהתאם לתקנה 2 לתקנות אבטחת מידע. על בעל מאגר מידע לבחון את הצורך בעדכון המסמך אחת לשנה לפחות ובכל פעם שנעשה שינוי משמעותי, כמפורט בתקנה. המסמך

	רמת האבטחה הבסיסית	רמת האבטחה הבינונית	רמת האבטחה הגבוהה	מאגר המנוהל בידי יחיד
התקנות החלות	תקנות 1-3	תקנות 1-4	תקנות 1-20	תקנות 1-2
	4(א), (ב), (ג), (ה), (ו)	5(א), (ב), (ה)		6(א)
	5(א), (ב), (ה)	15-6		9(א)
	6(א)	16(ב), (ג), (ה)		11(א)
	7(א), (ב)	17		14-12
	8	18(א)		20
	9(א), (ג)	19		
	11(א), (ב)	20		
	15-12			
	17			
	19			
	20			

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

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

ג. **חובת הרשות המקומית לקבוע, במסמך ברור, נוהלי אבטחת מידע, שמטרתם לייצר מדיניות אבטחת מידע עקבית בארגון**, כך שניתן יהיה להתמודד עם סיכוני אבטחה אליהם חשוף המידע. חובה זו מוגדרת בתקנה 224.

ד. **הרשות המקומית מחויבת לבצע מיפוי של מערכות המאגר וכן סקר סיכונים**. כלומר, להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת פרטים כמו: תשתיות ומערכות חומרה, סוגי רכיבים, תוכנות, ממשקים וכן פרטים נוספים המובאים בהרחבה בתקנה 5 במדריך המלא. **מאגר עליו חלה רמת האבטחה הגבוהה מחויב לערוך סקר לאיתור סיכוני אבטחת מידע** (סקר סיכונים) **אחת ל-18 חודשים לפחות** ולפעול לתיקון ליקויים, אם התגלו. כמו כן, על מאגרים אלה חלה חובה לבצע **מבדקי חדירות** אחת ל-18 חודשים לפחות, לבחינת עמידותם.

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

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

ז. **הרשות המקומית מחויבת לוודא שעובדים להם קיימת גישה למאגר הם אכן עובדים המורשים לכך, וזאת באמצעות זיהוי ואימות** (לכל הפחות באמצעות סיסמא). כמו כן, נדרש

22 דגשים ספציפיים לכתיבת ולשמירת הנוהל מובאים בהרחבת באתר הרשות להגנת הפרטיות.

לנהל מנגנון המתעד באופן אוטומטי ועצמאי כל גישה למערכת, עליו תבוצע בקרה תקופתית, כמפורט בתקנות 9 ו-10 לתקנות ובמדריך המלא.

ח. **חובתה של הרשות המקומית לתעד אירועי אבטחה שהתרחשו, על מנת לייצר זיכרון ארגוני ביחס לאירועים חריגים ולהפיק מהם לקח לעתיד**. תקנה 11 לתקנות מגדירה מהו 'אירוע אבטחה חמור' כשמדובר במאגר עליו חלה רמת האבטחה הגבוהה ומהו אותו אירוע כשמדובר ברמת אבטחה בינונית. במקרה של "אירוע אבטחה חמור", **מחויבת הרשות המקומית להודיע לרשות להגנת הפרטיות באופן מיידי על כך**, וכן לדווח על הצעדים שננקטו בעקבות האירוע. ניתן לדווח באופן מקוון באתר האינטרנט של הרשות.

ט. **הרשות המקומית מחויבת להקפיד על מניעת זליגת מידע בעת שימוש בהתקנים ניידים** (מחשבים ניידים, טלפונים חכמים וכד'), במידת הצורך האמצעות הגבלת חיבור המאגרים להתקנים ניידים (תקנה 12). כמו כן, יש **להקפיד על ניהול מאובטח ומעודכן של מערכות המאגר** (תקנה 13). בנוסף, במידה ומערכות המידע והמאגרים מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, **מחובת הרשות המקומית לנקוט באמצעי אבטחה נוספים שימנעו גישה חיצונית ולא מורשית למידע** (תקנה 14).

י. **חובת הרשות המקומית לנקוט משנה זהירות כאשר מוענקת גישה למאגרי המידע לגורמים חיצוניים בהתקשרות באמצעות מיקור חוץ**[23] (כמפורט להלן בהתייחסות לתסקיר בפרק 5 במדריך זה[24]), עוד בטרם התקשרות במיקור חוץ יש לבחון את סיכוני אבטחת המידע האפשריים, ובמידה והם גבוהים מידי יש להימנע ממיקור חוץ (ראו פירוט בפרק 6 למדריך זה). כמו כן, יש לקבוע בהסכם מפורש עם הספק החיצוני קווים מנחי לפעילותו, בין היתר: סוג המידע אותו רשאי לעבד, מערכות אליהן רשאי לגשת, חובתו לסודיות ועוד (כמפורט בתקנה 15 וכן בהנחיית הרשות להגנת הפרטיות בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי).

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

יב. **הרשות המקומית מחויבת להקפיד על משך זמן שמירת נתוני האבטחה ועל גיבוי ושחזור נתוני אבטחה**, שיש לבצע אחת לתקופה ובהתאם לדגשים המובאים בתקנות 17-18.

יג. חשוב לזכור כי **חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל המאגר, על מנהל המאגר ועל מחזיק המאגר**. כמו כן, מוזכר כי לרשות להגנת הפרטיות שמורה הזכות לפטור מאגרים ספציפיים מחובות אבטחת מידע מתוך התקנות, או לחלופין להטיל חובות נוספות בהתאם לנסיבות, כמפורט בתקנות 19-20.

23 הרשות להגנת הפרטיות מנחה גם לעניין זה.

24 "מדריך הגנת הפרטיות לעיר החכמה" של הרשות להגנת הפרטיות - קישור אליו מופיע לעיל.

75. ככלל, מאחר שהמועצה היא גוף ציבורי, מדובר במאגרים שחל עליהם רמת אבטחה בינונית. לצורך המחשת חשיבות הנושא במועצה האזורית, להלן ציטוט של סעיף 16 לתקנות הגנת הפרטיות:

> 16. (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר אחראי לכך שתיערך, אחת ל-24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.
>
> (ב) בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.
>
> (ג) בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

מטרות הביקורת

- לבחון תפקוד המועצה בנוגע לאבטחת המידע.
- לבחון עמידת המועצה בדיני הגנת הפרטיות החלים עליה ובתחום אבטחת המידע.
- להצביע באופן כללי על סיכונים פוטנציאליים.
- להביא בדוח ממצאים ולחשוף סיכונים וחולשות.
- להביא בדוח המלצות לתיקון הליקויים.

היקף הביקורת

הביקורת בדקה את עמידת המועצה בעיקרי דיני הגנת הפרטיות החלים עליה, בהנחיות הרשות להגנת הפרטיות ובכללי בסיס - בשנת 2022. כמו כן, הביקורת בחנה תיקון ליקויים במספר נושאים מביקורת קודמת בנושא.

הדוח מתמקד בנושאים הבאים:

א. מסמך הגדרות מאגר
ב. רישום מאגרי מידע
ג. חובת מבקש מידע, זכות העיון ותיקון מידע
ד. נהלי אבטחת מידע
ה. מסירת מידע או ידיעות מאת גופים ציבוריים
ו. ועדת היגוי לתחום אבטחת המידע
ז. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב
ח. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות
ט. הדרכה וקיום אבטחת מידע אצל עובדים
י. חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת
יא. שמירה, גיבוי ושחזור של נתוני אבטחה
יב. רישוי תוכנות
יג. אבטחה פיזית וסביבתית
יד. ניהול הרשאות גישה וזיהוי ואימות
טו. חיבור התקנים
טז. בקרה ותיעוד גישה
יז. תיעוד של אירועי אבטחה
יח. עיר חכמה
יט. מיקור חוץ

כ. מינוי ממונה אבטחת מידע
כא. מינוי ממונה הגנה על הפרטיות

בביקורת הקודמת, הדוח התמקד בנושאים הבאים:

א. נהלים
ב. קיום מסמך הגדרות מאגר,
ג. רישום מאגרי מידע,
ד. ממונה ואחראי אבטחת מידע (ועדת היגוי לתחום אבטחת המידע)
ה. קיום נהלי אבטחת מידע,
ו. מיפוי מערכות המאגר,
ז. ביצוע סקרי סיכונים,
ח. אבטחה פיזית וסביבתית,
ט. ניהול הרשאות גישה וזיהוי ואימות,
י. הגבלת השימוש בהתקנים ניידים,
יא. בקרה ותיעוד גישה,
יב. תיעוד של אירועי אבטחה,
יג. הסכמים עם גורמים חיצוניים,
יד. שעון נוכחות ביומטרי.
טו. מצלמות – מדגם.
טז. תקצוב אבטחת מידע
יז. ממונה הגנת הפרטיות
יח. הדרכה וקיום אבטחת מידע אצל עובדים
יט. הדרכה וקיום אבטחת מידע אצל נותני שירות ומיקור חוץ (outsourcing)
כ. תחום הגיבוי – הגופים החיצוניים והמועצה
כא. חומת אש (FireWall), ואנטי וירוס
כב. רישוי תוכנות
כג. אתר האינטרנט של המועצה
כד. אבטחה פיזית
כה. מערכות אל-פסק
כו. בטיחות אש ומים
כז. אבטחה לוגית
כח. ניטור יומן השימוש - (log)
כט. סיסמאות
ל. אבטחת מידע במחשבים מנותקי רשת ובהתקני אחסון ניידים
לא. תוכנית שיקום מאסון ותוכנית המשכיות עסקית
לב. מחלקות: מדגם

במסגרת דוח זה, נבדק גם תחום תיקון הליקויים בחלק מהנושאים. מחמת הזמן הרב שעבר, פרסום תקנות אבטחת המידע החדשות, עדכוני נהלים והנחיות, חלק מהדברים אינו רלבנטי ולכן לא עלה צורך בבדיקה מעמיקה בבדיקת תיקון כל הליקויים.

מתודולוגיה – שיטת הביקורת

במסגרת הביקורת ננקטו הפועלות הבאות:

א. קיום פגישות עם מנהל מחלקת מערכות מידע / ממונה אבטחת המידע, עובדים וחלק ממנהלי מחלקות בהן מנוהל מידע פרטי.

ב. לימוד מיפוי מחשוב המועצה על כל עמדות העבודה לפי סקר מקצועי.

ג. בדיקה וסקירת עמדות העבודה מבחינת רישוי תוכנות במועצה וקיום התקנת אנטי וירוס בסיסי לפי סקר מקצועי.

ד. סקירת מסמכים ודוחות שהופקו ממערכות המועצה.

ה. ביקורים וראיונות במחלקות.

ו. ביקורים באתרים שונים במתחם המועצה כולל חדר השרתים.

ז. סקירת מספר עמדות עבודה אישיות ממוחשבות, ניסיונות חדירה פשוטים.

ח. עיון בהסכמים של מיקור חוץ.

ט. בדיקת מצב נתון מול חקיקה, תקנות, נהלים, כללים ותקנים מקצועיים.

י. היוועצות בגורמים מקצועיים.

הביקורת נערכה על פי תקני ביקורת מקובלים.

פרק ד' ממצאים והמלצות

מידע כללי

במחלקות המועצה מנוהל מידע אישי רגיש, לצורך הדוג':

א. מחלקת הרווחה – נתוני מטופלים

ב. מחלקת החינוך – נתוני קטינים

ג. שפ"ח – נתוני קטינים מטופלים

ד. מחלקת הגביה – נתוני תושבים

ה. מחלקת משאבי אנוש ומחלקת השכר – פרטים אישיים אודות עובדים לרבות שכרו ומאגר ביומטרי

ו. המוקד העירוני – הקלטות של פניות תושבים

ז. מצלמות אבטחה – צילומים

סקר מקצועי למיפוי מחשוב, רשת, ורישוי

נתוני המועצה בתחום פריסת המחשוב, הינה במבנים פיסיים כדלקמן:

- בניין משרדים ראשי כולל לשכת ראש המועצה, מנכ"ל, גזברות, הנהלת חשבונות, חינוך, רכש, ביטחון ועוד.
- מחלקת הנדסה והוועדה לתכנון ולבניה
- מבני תחזוקה.
- ספריה.
- רווחה.
- גביה.
- אולם ספורט.

לבקשת הביקורת, ממונה אבטחת המידע ערך והציג סקר מקצועי למיפוי מחשוב, רשת, ורישוי (חסוי)

פירוט הממצאים וההמלצות

1. מסמך הגדרות מאגר

תקנה 2 לתקנות אבטחת מידע קובעת, כי על בעל מאגר מידע להגדיר את המאגר במסמך הגדרות מאגר:

(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.

(ב) בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד 31 בדצמבר.

(ג) בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

ממצאים

המועצה לא מיפתה את מאגרי המידע הרלוונטיים לחוק הגנת הפרטיות ולא הוכנו מסמכי "הגדרת מאגר" כנדרש בתקנות.

המלצות

עריכת מסמך הגדרת המאגר, תסייע למועצה להגדיר מהי רמת האבטחה החלה עליה, שלה תלות במספר בעלי ההרשאה למאגרי המידע במועצה, במספר האנשים עליהם שמור מידע במאגרים ובאופי המידע השמור.

על המועצה, המנהלת מאגרי מידע על תושביה, הכוללים אפיון נושאי המידע לרבות מידע עליהם, לבצע מיפוי לכל מאגרי המידע הקיימים אצלה, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים ולעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

2. רישום מאגרי מידע

בסעיף 8 (א) לחוק הגנת הפרטיות נקבע כי:

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.

(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

(ג) בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

(1) מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;

(2) יש במאגר מידע רגיש;

(3) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;

(4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;

(5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.

סעיף 9 לחוק מגדיר את אופן הגשת הבקשה לרישום מאגר מידע אצל הרשם.

ממצאים

משיחות עם עובדי מועצה וממונה אבטחת המידע נמסר, כי אין מאגרים רשומים או כי לא ידוע על כאלה. הרשות להגנת הפרטיות מסרה, כי קיימים חמישה מאגרים רשומים. מסתבר שהרישום לוקה בחסר, אינו מעודכן ומכיל פרטים לא נכונים. להלן שמות המאגרים וחלק מהפרטים:

א. תיקים אישיים בהנהלת חשבונות. לא רשום שם מנהל מאגר. נרשם בשנת 2011.

ב. גביה. נרשם בשנת 2011. כמנהל המאגר רשום שם של גזבר המועצה שהפסיק את תפקידו בשנת 2005 (לפני כ-17 שנים). לא ברור כיצד המאגר נרשם על שמו.

ג. שכר ומשאבי אנוש. נרשם בשנת 2013. כמחזיקה רשומה החברה לאוטומציה.

ד. שכר וכח אדם. נרשם בשנת 2011. כמנהלת המאגר רשומה עובדת מועצה שפרשה בשנת 2017.

ה. מערכת פיננסית. נרשם בשנת 2013. לא רשום מנהל מאגר. כמחזיקה רשומה החברה לאוטומציה.

מלבד המאגרים הנ"ל שרישומם לא מעודכן, המועצה טרם רשמה את מאגרי המידע אצל רשם המאגרים כנדרש בסעיף 8 בחוק.

יצוין, כי משיחת הביקורת עם נציגי הוועדים המקומיים, עולה כי אין מודעות לחובות הוועדים בתחום מאגרי המידע ובכלל בתחום אבטחת המידע. ניתן לומר כבר כאן, כי בכל נושא שבו מתואר כשל של המועצה בתחום אבטחת המידע, הדברים נכונים גם לגבי הוועדים המקומיים בתחום חובותיהם לפי דין.

המלצות

רישום המאגרים נועד להבטיח את הגנת הפרטיות של מאגרי המידע ולתת כלים, הן לרשם מאגרי המידע והן לציבור שהמידע עליו מנוהל במאגרי המידע, וכך ניתן לאכוף את הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי המאגרים.

במצב בו אין נהלים ואין יישום של הדין בנושא, מומלץ, כי המועצה תבחן מה עליה ליישם מדיני הגנת הפרטיות, תמפה את מאגריה ותפעל בהתאם לכל הוראות הדין.

כך וכאמור, על בסיס המיפוי הנדרש כאמור לעיל, על המועצה לרשום מאגרי מידע שאינם רשומים, לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע וכו'.

ההמלצה האמורה נכונה גם לגבי הוועדים המקומיים שעליהם לוודא את קיום הוראות הדין בתחום מאגרי המידע ובכלל בתחום אבטחת המידע. הדברים לגבי הוועדים מוזכרים כאן, אך נכונים לאורכו של הדוח.

3. חובת מבקש מידע, זכות העיון ותיקון מידע

סעיף 11 לחוק הגנת הפרטיות עוסק בחובת מבקש המידע וקובע:

פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה –

(1) אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו;

(2) המטרה אשר לשמה מבוקש המידע;

(3) למי יימסר המידע ומטרות המסירה.

יוער, כי הרשות להגנת הפרטיות פרסמה מסמך המציג את עמדת הרשות בנושא חובת היידוע במסגרת איסוף ושימוש במידע אישי.

בהתאם לפרסום הרשות באתרה:25 המסמך מבהיר כי חובת היידוע הקבועה בסעיף 11 לחוק הגנת הפרטיות חלה בכל מקום בו איסוף מידע אישי על אודות אדם נעשה על יסוד פנייה אליו, וזאת בין אם המידע נאסף מכוח הסכמת נושא המידע, ובין אם איסוף המידע נעשה מכוח הסמכה שבדין.

הרשות הבהירה, כי איסוף מידע מאדם ושימוש בו ללא יידוע מספק של נושא המידע משליך על תוקף ההסכמה מדעת, ועשוי להוות הפרה של הוראות חוק הגנת הפרטיות. ככל שהמידע הנאסף הוא רגיש במיוחד, וכאשר קיים חשש אינהרנטי שהסכמת נושא המידע עלולה להיות מוגבלת, רצוי כי חובת היידוע תהיה רחבה יותר מהקבוע בסעיף 11 לחוק.

הזכות לפרטיות הינה זכות חוקתית המעוגנת בחוק יסוד: כבוד האדם וחרותו. בין היתר מדובר בחירות הבסיסית "להיעזב במנוחה" ואת זכותו של האדם לשלוט במידע אישי על אודותיו.26

חובת היידוע על המידע האישי הכללית והן זו הקבועה בסעיף 11 הנ"ל, נובעת גם מהמאפיינים הייחודיים של הזכות לפרטיות. הזכות לפרטיות קשה להגדרה, גבולותיה לא תמיד ברורים, ועלולים להיגרם נזקים (קשים לכימות) כתוצאה מפגיעה בה.

25 הדברים שלהלן מתוך אתר הרשות בכתובת: https://www.gov.il/he/departments/news/duty_to_notify המסמך פורסם בתאריך 31.07.2022.

26 בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת** בפסקאות 10 ו- 13 לפסק דינה של השופטת דפנה ברק-ארז.

בשני מצבים הדין מתיר איסוף ושימוש במידע אישי על אודות אדם: האחד מכוח הסכמת האדם נושא המידע, והשני, כאשר האיסוף והשימוש נעשים מכוח הסמכה חוקית. בשני המצבים הדין מחייב את הגורם המבקש לאסוף ולהשתמש במידע ליידע את נושא המידע על כך, ולפרט בפניו נתונים הנוגעים לאיסוף ולשימוש במידע על אודותיו.

מתוך תמצית המסמך של הרשות להגנת הפרטיות:

"חובת היידוע הקבועה בהוראות סעיף 11 לחוק הגנת הפרטיות חלה בכל מקום בו איסוף מידע אישי על אודות אדם נעשה על יסוד פנייה אליו, וזאת בין אם המידע נאסף מכוח הסכמת נושא המידע, ובין אם איסוף המידע נעשה מכוח הסמכה שבדין. חובה זו חלה גם כאשר הפנייה לאדם לקבלת מידע נעשתה בעקבות בקשתו של אותו אדם לקבלת שירות מסוים.

על-פי הוראות סעיף 11, גורם המבקש לאסוף מידע אישי מאדם צריך לפרט, בעת הפניה לאותו אדם, איזה מידע ייאסף עליו, למי המידע עשוי להיות מועבר, ולשם איזו מטרה .

ככלל, איסוף מידע מאדם ושימוש בו ללא יידוע מספק של נושא המידע, משליך על תוקף ההסכמה מדעת, ועשוי להוות הפרה של הוראות חוק הגנת הפרטיות. במצבים בהם חובת היידוע מיושמת כחלק מהליך קבלת ההסכמה מדעת, היקפה של חובת היידוע עשוי להיות מושפע מהדרישות לשם קבלת ההסכמה. כך, נתונים שונים כגון זהות מבקש הבקשה, אופי מערכת היחסים שלו עם נושא המידע ומידת יכולתו של נושא המידע להתנגד לבקשה, וכן סוג ורגישות המידע, עשויים להביא להרחבה של חובת היידוע הנדרשת.

היידוע צריך להיות בשפה ברורה, פשוטה ונגישה, להינתן בד בבד עם הפניה לאדם, ומומלץ כי יכלול פירוט בדבר אופן שמירת המידע (כגון זהות מורשי הגישה למידע), ובדבר זכויותיו של נושא המידע. ככל שהשירות מופנה לציבור מובחן מבחינה מסוימת (כגון גיל, ארץ מוצא או מוגבלות), חשוב ששפת היידוע תהיה מותאמת, ככל האפשר, והדבר יכול להשליך גם על תוקף ההסכמה מדעת. עם זאת יובהר כמובן שבמצב בו קיימים הסדרים חוקיים או רגולטוריים סותרים בנוגע לאופן יישום חובת היידוע בנסיבות ספציפיות או ביחס לגורמים ספציפיים (כגון בנקים וכו'), הסדרים אלו עשויים לגבור, ואפשר שיהיה על הגורמים הרלוונטיים לפעול לפיהם.

ככל שהמידע הנאסף הוא רגיש במיוחד (כגון מידע ביומטרי) ובנסיבות בהן קיים חשש אינהרנטי כי הסכמת נושא המידע עלולה להיות מוגבלת, רצוי לכלול במסגרת היידוע פרטים נוספים הנוגעים לאיסוף המידע, ולאופן ומטרות השימוש בו.

כאשר בעל מאגר מתקשר עם גורם חיצוני לצורך קבלת שירות במסגרת 'מיקור חוץ' בהתאם להוראות תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'תקנות אבטחת מידע'), והגורם החיצוני מבקש להשתמש במידע האישי שנאסף על-ידו במסגרת מתן השירות למטרות השונות ממטרת השירות המקורי, על הגורם החיצוני ליידע את נושא המידע על כך, ולבקש את הסכמתו".

סעיף 13 לחוק עוסק בזכות העיון במידע וסעיף 14 בנושא תיקון המידע.

<u>ממצאים</u>

ככלל, בתחומים שונים כמו חינוך, רווחה וגביה, המועצה אינה מקפידה על שקיפות בנוגע למקור הסמכות לאיסוף המידע האישי על התושבים, ואינה מקפידה על יידוע התושבים שעליהם מוחזק המידע בדבר זכויותיהם בנוגע למאגר המידע בו נשמרים פרטיהם, בהתאם לסעיף 11 לחוק בעת פניה לקבלת מידע מהתושב. לא נמצא יידוע לתושבים ולנושאי המידע בדבר האפשרות לעיין במידע כנדרש בסעיף 13 לחוק ולא בדבר האפשרות לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק.

המלצות

על המועצה ליידע את התושבים בדבר המקור החוקי לאיסוף המידע אודותיהם, וכאשר אין סמכות חוקית כזו, לקבל את הסכמת התושב עבור שמירת פרטיו במאגריה. זאת, עם מתן הודעה לתושבים בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה עליהם חובה חוקית למסור את המידע כאמור, או שהיא נתונה לרצונם והסכמתם, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע והמטרה. כמו כן, על המועצה להקפיד לאפשר לתושבים לעיין במידע אודותיהם, בהתאם להוראת סעיף 13 לחוק. זכות עיון זו חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות למוקד, פניות לאתר, שיחות זום ואחרות מצולמות בווידאו

וכיו״ב או שמירת צילומים אחרים, אשר נשמרים באופן דיגיטלי על ידי המועצה או גוף אחר הנותן שירות לציבור. כמו כן, יש להקפיד ולאפשר לתושבים לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע בהתאם לסעיף 14 לחוק, כאשר המידע אינו נכון, שלם, ברור או מעודכן.

4. נהלי אבטחת מידע

- בתקנה 3(2) לתקנות אבטחת המידע נקבע, כי הממונה על אבטחת המידע יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר. תקנה 4 מפרטת את הנושאים שיש לעסוק בהם במסגרת נוהל האבטחה.
- נהלים בתחום אבטחת המידע הם בסיס לעבודה נכונה בתחום.
- מלבד המצוי בדין, ניתן ללמוד רבות מהנהלים הקיימים בגופים שונים על חשיבות ויישום אבטחת מידע ברמה גבוהה ועל נהלים שניתן לאמץ בהתאמות הנדרשות וללא הכבדה יתרה.

- בתקנות 4(א) ו-4(ב) לתקנות אבטחת המידע נקבע:

(א) בעל מאגר המידע יקבע במסמך נוהל אבטחת מידע (להלן – נוהל האבטחה) בהתאם למסמך הגדרות המאגר ותקנות אלה, אשר יחייב כל בעל הרשאה בהתאם לפרטים מהנוהל שאליו הוא חשוף לפי תקנת משנה (ב).

(ב) בעל מאגר מידע ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

בתקנות 4(ג) ו4(ד) לתקנות אבטחת המידע נקבע מה בין השאר יש לכלול בנוהל האבטחה. עיקרי הדברים בטבלה שלהלן:

מס״ד	התקנה	פירוט הדרישה
כלל המאגרים		
1	4 (ג) (1)	הוראות בעניין אבטחה פיזית וסביבתית של אתרי המאגר בהתאם לתקנה 6 (א) ו-(ב)

מס״ד	התקנה	פירוט הדרישה
2	4 (ג) (2)	הרשאות גישה למאגר ולמערכות המאגר בהתאם לתקנה 8
3	4 (ג) (3)	תיאור האמצעים שמטרתם להגן על המאגר ועל מערכות המאגר
4	4 (ג) (4)	הוראות למורשי הגישה למאגר ולמערכות המאגר
5	4 (ג) (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
6	4 (ג) (6)	אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11, לפי חומרת האירוע ומידת רגישות המידע
7	4 (ג) (7)	הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12
13	4 (ה)	בחינת הצורך בעדכון נוהל אבטחת מידע בתדירות של אחת לשנה לפחות
מאגרי מידע בעלי רמת אבטחה בינונית או גבוהה		
8	4 (ד) (1)	אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9
9	4 (ד) (2)	פירוט אופן הבקרה על השימוש במאגר המידע לרבות תיעוד הגישה למערכות המאגר, בהתאם לתקנה 10
10	4 (ד) (3)	הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של

מס"ד	התקנה	פירוט הדרישה
		אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16
11	4 (ד) (4)	הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א)(1)
12	4 (ד) (5)	הוראות לאופן ביצוע פעולות פיתוח ותיעודן, לרבות הרשאות גישה לאנשי הפיתוח

בתקנות 4(ה) ו-4(ו) לתקנות אבטחת המידע נקבע:

(ה) בעל מאגר מידע יבחן, אחת לשנה, את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור, יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה:

(1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע;

(2) נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

(ו) ארגון שהוא בעל כמה מאגרי מידע רשאי לקבוע נוהל אבטחה כאמור בתקנה זו, במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.

ממצאים

במועצה לא קיימים נהלי עבודה בנושא אבטחת מידע כנדרש בתקנות. יצוין, כי כבר בשנת 2015, לפני כניסתן לתוקף של תקנות אבטחת המידע, הביקורת המליצה לקבוע נוהל שיכלול בעיקר את המרכיבים הבאים:

- מבנה מאגר המידע ורשימת מצאי;
- תיאור אמצעי ההגנה על מערכות המחשוב ותשתיות התקשורת;
- סמכות ואחריות;
- הדרכה והוראות למורשי גישה למערכת, לגבי אופן השימוש במערכת תוך אבטחת המידע;
- תיאור רכיבי המערכות ותיאור מבנה הרשת;
- הסיכונים להם חשוף המידע;
- תיאור אופן מתן הרשאות גישה למערכת ואופן ביטולן;

- הוראות בדבר אופן אימות זהותם של מורשי גישה למערכת ואופן הטיפול בתקלות באימות זהות;
- הוראות לעניין רמת אבטחת הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות;
- הוראות בדבר אבטחה פיזית וסביבתית;
- ניתור ובקרה על שימוש במערכות המידע; הוראות בדבר עבודה עם גורמי חוץ;
- הוראות בדבר ניהול והעברה של אמצעי אחסון והתקנים ניידים;
- הוראות בדבר אופן גיבוי מידע, שחזורו ואופן התמודדות עם אירוע אבטחה;
- הוראות בדבר ביצוע ביקורות תקופתיות וסקר סיכונים לשם הבטחת קיומם ותקינותם של אמצעי האבטחה; אופן התמודדות עם אירועי אבטחה;
- הוראות בדבר חובת דיווח למנהל על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.
- תוכן הנוהל שהוצע, התבסס, בין השאר, על גרסת טיוטה של תקנות אבטחת מידע לפני שנכנסו לתוקף. הומלץ למועצה ללמוד מטיוטת התקנות, אך הדבר לא נעשה.

המלצות

על המועצה להכין ולהסדיר נוהל מפורט בהתאם לדין, ומומלץ שאף מעבר לו בנושא אבטחת המידע ולעדכנו מעת לעת לפי הצורך.

עובר לקביעת הנהלים, מומלץ להיוועץ בגורמי מקצוע ולקבוע מדיניות אבטחה.

5. מסירת מידע או ידיעות מאת גופים ציבוריים

במקרים מסוימים שיתוף מידע אישי אודות אנשים בין גופים ציבוריים שונים הוא כלי חשוב לייעול השירות, אך גם עלול לפגוע בפרטיות. לאור זאת, פרק ד' לחוק הגנת הפרטיות עוסק במסירת מידע או ידיעות מאת גופים ציבוריים (סעיפים 23-23ז). העברת מידע בין גופים ציבוריים בניגוד לחוק, מהווה עבירה פלילית לפי סעיף 31א(א)(8) לחוק הגנת הפרטיות.

מסירת מידע מאת גוף ציבורי לפי סעיף 23ב לחוק זה אסורה למעט במקרים הבאים:

- המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין.
- האדם אשר המידע מתייחס אליו נתן הסכמתו למסירה.

- קבלה או מסירה של מידע בידי רשות בטחון, כמשמעותה בחוק, לשם מילוי תפקידה, ובלבד שהמסירה או הקבלה לא נאסרה בחיקוק.
- מסירת המידע היא בין גופים ציבוריים ועומדת בתנאים המוגדרים בפרק ד' לחוק הגנת הפרטיות.

בהתאם לסעיף 23ז לחוק הגנת הפרטיות, הותקנו תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסידרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986.[27]

בתקנות נקבעו נהלי ביצוע העברת מידע בין גופים ציבוריים וכן סדרי ניהול מאגר המכיל מידע מוגבל וכללי השימוש בו. בין היתר נקבע, כי המנהל הכללי של גוף ציבורי ימנה ועדה להעברת מידע לפי פרק ד' לחוק. על הוועדה לבחון בקשות למסירת המידע מאת הגוף הציבורי וכן לבחון בקשות לקבלת מידע של הגוף הציבורי מאת גוף ציבורי אחר. כמו כן, על הוועדה לקבוע הוראות לעניין ההרשאות וההגבלות בעניין הגישה למאגרי המידע.

על מנת להמחיש את חשיבות עבודת הוועדה, להלן דברים שפרסמה הרשות להגנת הפרטיות באשר לבחינת בקשות על ידי הוועדה להעברת מידע:

"כיצד נבחנות בקשות לקבלת מידע על ידי הוועדה להעברת **מידע?**

- בקשה לקבלת מידע של גוף ציבורי תועבר לאישור הוועדה להעברת מידע לאחר שבעלי התפקידים באותו גוף ציבורי אישרו את המצוי בתוספת לתקנות, אך זאת טרם להעברת הבקשה לגוף הציבורי ממנו נתבקש המידע.
- על הוועדה לבחון כי המידע המבוקש אכן נדרש, ובאופן בו הוא נתבקש, וכי מובטח שהגישה למידע תהיה מצומצמת ומפוקחת

כיצד נבחנות בקשות למסירת מידע על ידי הוועדה להעברת מידע?

- **עמידה באישורים הנדרשים בתקנות** -על הוועדה להעברת מידע לבחון האם הבקשה הוגשה על גבי טופס א' אשר אושר על ידי כל הגורמים רלבנטיים בגוף המבקש את המידע (מנהל מאגר המידע, הממונה על האבטחה, היועץ המשפטי והוועדה).

- **מעמדו של הגוף מבקש המידע** -על הוועדה לבחון כתנאי מקדים האם מדובר בגוף ציבורי כהגדרתו בסעיף 23 לחוק.

- **האם קיימת מניעה למסירת המידע** -על הוועדה לבחון האם מסירת המידע לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית והאם לא הותנתה מסירתו

27 בהמשך, בעקבות פסיקת בית המשפט העליון בבג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**, פ"ד נח(4) 842 – בה נקבע כי על רשויות המדינה להגביר את הפיקוח על הגישה למאגרי המידע ועל היקף המידע המועבר בין גופים ציבוריים – תוקנו התקנות העיקריות, ועוגנה בהן חובת הקמתה של ועדה להעברת מידע בכל גוף ציבורי.

בכך שהמידע לא יימסר לאחר.

- **תנאי מסירת המידע** -קיימת הבחנה בתנאי מסירת המידע בין בקשות לקבלת מידע מאת משרד ממשלתי או מוסד מדינה לבין בקשות לקבלת מידע מיתר הגופים הציבוריים (סעיף 23ג לתקנות).
  - **כאשר הבקשה לקבלת מידע היא מאת משרד ממשלתי או מוסד מדינה** -על הוועדה לבחון האם מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכותית או התפקידים של מוסר המידע או מקבלו.
  - **כאשר הבקשה למסירת מידע היא מאת גוף ציבורי אחר** -על הוועדה לבחון האם מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע והאם היא דרושה למטרת ביצוע חקיקה או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו. או לחלופין, האם הגוף הציבורי אשר ביקש את המידע רשאי לדרוש את אותו המידע על פי דין מכל מקור אחר.

- **מידתיות וסבירות** -על הוועדה לבחון את מידתיות וסבירות הבקשה בהתייחס לרגישות המידע אותו מעוניינים להעביר, ולכך כי ככל שהמידע רגיש יותר יש צורך בהגנה רבה יותר על הפרטיות, תוך בחינת האלמנטים הבאים:
  - האם הבקשה מתאימה ליישום המטרה לשמה נדרש המידע ויש קשר הגיוני ביניהן .
  - האם העברת המידע באופן המבוקש היא אמצעי פחות פוגע מבין מגוון האמצעים למימוש אותה המטרה.
  - האם קיים יחס סביר בין המטרה לבין הפגיעה שנגרמת בזכות לפרטיות לשם השגתה.

- **אמצעי האבטחה של מאגר המידע** -על הוועדה לבחון את אמצעי האבטחה של מאגר המידע בגוף המקבל את המידע בשלושה היבטים:
  - אמצעי מחשוב - סיסמאות כניסה למערכת, מידור בתוך מאגר המידע בין פרטי מידע שונים, אמצעי הגנה על חדירה מבחוץ וכד ;'
  - אמצעים פיסיים - מיקום המאגר, הגישה הפיסית אליו וכד ;'
  - אמצעי בקרה - תדירות הבדיקות שנעשו למניעת חדירה למאגר המידע מבחוץ, אופן הפיקוח על השימוש שנעשה במידע על ידי מורשי הגישה וכד.'

- **מורשי הגישה למידע** -על הוועדה לבחון מי יהיו בעלי התפקידים שתינתן להם רשות לעיין במידע שנמסר, מספרם ולצורך איזו מטרה ניתנת להם הגישה למידע.

- **טיפול במידע עודף** -על הוועדה לבחון כיצד משמידים מידע עודף אשר נמסר באופן נלווה לבקשה העיקרית ומה עושים במידע ישן, אשר אין בו עוד שימוש".[28]

ממצאים

במועצה לא מיושמים הכללים בדבר מסירת מידע או ידיעות מאת גופים ציבוריים.

המלצות

מומלץ, כי המועצה תקבע מדיניות והגדרות לגבי העברת המידע לגופים ציבוריים.

על המועצה ליישם באופן מיידי את הוראות החוק והתקנות בעניין מסירת מידע או ידיעות מאת גופים ציבוריים. מומלץ למועצה לוודא קיום הוראות הדין גם באשר למידע שמקבל אצלה מגופים אחרים.

6. ועדת היגוי לתחום אבטחת המידע

מדובר בנושא חוזר מדוח 2015 (כליקוי שלא תוקן וכמעט כלשונו). אומנם כיום נדרש ממונה אבטחת מידע, אך בארגונים רבים פועלות ועדות היגוי כפורום עם ראייה כוללת.

ברשות מקומית רצוי להקים ועדת היגוי לאבטחת מידע, שתבטיח את ביצוע אבטחת המידע מנקודת מבט כוללת וניהולית עם התוויית דרך נאותה, קידום נושאי אבטחה באמצעות מחויבות והקצאת משאבים מספיקים.

ועדת ההיגוי תעסוק בדרך כלל בנושאים הבאים:

א. סקירה, שיפור וקביעת מדיניות אבטחת מידע ואחריות כללית.

ב. אישור תוכנית עבודה שנתית בתחום אבטחת מידע, לרבות תקציבים, לוחות זמנים ותחומי אחריות.

ג. גוף מייעץ ומסייע להנהלת המועצה להבנה, למודעות ולקבלת החלטות נכונות.

ד. התוויית פעולות בהתאם ולשם עמידה בהוראות הדין וההנחיות.

28 משרד המשפטים, הרשות להגנת הפרטיות "העברת מידע בין גופים ציבוריים" https://www.gov.il/BlobFolder/service/information_flow_between_public_bodies/he/info-bulletin.pdf

ה. דיון באירועי אבטחה ופגיעה בפרטיות.

ו. שיפור וקידום יוזמות עיקריות לחיזוק אבטחת המידע.

ז. מול ממונה אבטחת המידע - קבלת דיווחים, בקרה ומעקב ביצוע.

ממצאים

במועצה אין צוות היגוי או צוות חשיבה כלשהו אשר עוסק באופן ממוקד בנושא אבטחת מידע.

ממונה אבטחת המידע פועל לעליית מדרגה בתחום המחשוב באופן כללי, בעיקר בתחום התשתית, שמהווה בסיס לשיפור נושא אבטחת המידע.

בתוך כלל הפעולות הוזכר נושא אבטחת המידע והממונה עמד על חשיבותו, אך הנושא לא תוקצב ולא טופל באופן ייעודי.

שיפור התשתיות במועצה מהווה תנאי הכרחי, אך לא מספיק לאבטחת המידע.

הביקורת מברכת על פעילות המועצה בתחומי התשתית, אולם לצורך אבטחת מידע נאותה יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים ייעודי.

מבדיקת פעולות המועצה בתחום התשתיות עולה, כי התשתיות המשופרות עשויות לסייע למועצה באפשרות לעלות מספר קומות בתחום אבטחת המידע. בין היתר, התשתיות המשופרות עשויות להגביר את רמת הקונקטיביות בין האגפים, להגביר ולאחד את רמת האבטחה, לשפר את תעבורת הנתונים ולבקרה, להוסיף שרתים ואמצעי אבטחה, לנהל את התחנות האישיות ולשלוט עליהן ברמה הנדרשת, וכן להתקין אמצעי ניטור ובקרה.

כל אלו לא ייעשו מעצמם. התשתיות המשופרות מהוות תנאי, אך אין בכך די. הביקורת לא מצאה מדיניות ותוכניות ארוכות טווח העוסקות בכל אלו. הביקורת לא מצאה גוף ניהולי העוסק בתחום ברמה הכוללת, מלבד ממונה אבטחת מידע, המועסק באופן מצומצם ביותר ושלא מספיק לראייה כוללת והתוויית מדיניות, שהוא בעלים של החברה שנותנת שירות (על כך להלן).

המלצות

אכן, תשתיות המחשוב והתקשורת המשופרות במועצה, מהוות קפיצת מדרגה גם בתחום אבטחת המידע, אך אין בכך די. לדעת הביקורת, על המועצה להמשיך ביתר שאת בפעולותיה גם בהתמקדות באבטחת המידע ושמירת הפרטיות.

כשם שבתחום הבטיחות בתחבורה אין די בתשתיות ראויות ויש צורך בראייה כוללת ופעולות בתחומים מגוונים על מנת להתמודד, לייעל ולשפר את הבטיחות, כך בתחום

אבטחת המידע, בנוסף לפעילות בתחום התשתיות, יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים מספיק.

מלבד הצורך במינוי ממונה אבטחת מידע מתאים ובהיקף העסקה ראוי, על אף שהחוק לא מחייב, הביקורת ממליצה להקים ועדת היגוי בליווי גורם מקצועי לצורך אבטחת מידע ושמירת הפרטיות, שתדון במכלול תחומי אבטחת המידע ברמה הניהולית הכוללת ובין השאר, בנושאים העולים בדוח זה.

מומלץ שוועדת ההיגוי תתווה מדיניות, תפעל להקצאת משאבים נאותה, תסקור את הקיים, לפעל לשיפור וייזום, תאשר תוכניות עבודה, תקבל דיווחים ותעקוב באופן שוטף אחר ביצוע.

7. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב

תקנה 3(3) לתקנות אבטחת המידע קובע כי:

> הממונה יכין תוכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;

במסמך תורת ההגנה הוגדרה אחריות הארגון להכנת תוכנית עבודה רב-שנתית להתגוננות של הארגון מפני אירועי סייבר. יש צורך במיפוי הסיכונים, לגבש מענה הגנתי, להכין וליישם תוכנית להפחתת הסיכונים. על הארגון להגדיר תחילה על מה הוא נדרש להגן, מהי רמת ההגנה הנדרשת בו, ובאילו תחומים עליו להשתפר כדי להגיע לרמה זו.

במתווה להקמה ולהפעלה של יחידות לניהול מערכות מידע ברשויות המקומיות שהכין משרד הפנים בינואר 2019 נקבע כי על הרשות המקומית להכין תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית, שלפיה תפעל יחידת מערכות המידע לביצוע רכש של ציוד, לפיתוח ולשדרוג של תשתיות קיימות ולהתקשרות עם גורמים במיקור חוץ להשגת יעדי התוכנית. לפי המתווה, את תוכנית העבודה האסטרטגית יש ליישם לאחר מיפוי המצב הקיים ברשות בכל תחומי האחריות של היחידה לניהול מערכות מידע, כמו תשתיות תקשורת, שרתים, רשתות, מערכות מידע וכלים דיגיטליים, וכן השירותים הדיגיטליים, אבטחת המידע, ניהול מאגרי המידע וההגנה על הפרטיות. כך גם, יש לבצע איתור של צורכיהן הטכנולוגיים של היחידות השונות ברשות על מנת לברר מה נדרש להן, מהבחינה הטכנולוגית, כדי שיוכלו ליישם את תוכניות העבודה שלהן ולממש את החזון המקצועי שלהן.

ממצאים

במועצה לא הוכנה תוכנית לבקרה שוטפת על העמידה בדרישות התקנות. מנהל מערכות המידע מסר, כי בתכנון להכין תוכנית מקפת הן בתחום הרכש וההצטיידות והן בתחום אבטחת המידע. הדברים ייצאו לפועל לאחר אישור המועצה.

הגם שחלק זה לא מיועד לשעת חירום, יוער, כי לא הוכנה בידי בעלי מקצוע בתחום המחשוב תוכנית לשעת חירום בתחום אירועי הסייבר.

המלצות

על המועצה באמצעות ממונה אבטחת המידע להכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, להוציא אותה לפועל ולהודיע כאמור על הממצאים.

כמו כן, מומלץ למועצה לפעול בהתאם להנחיות תורת ההגנה ובכלל זה קביעת תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית עם כל הפעולות הנלוות כאמור.

מעבר לתוכניות השונות העולות בדוח זה שעל המועצה להכין, על המועצה להכין תוכנית לשעת חירום בתחום אירועי הסייבר.

מלבד עמידה בהוראות הדין, בנושאים שונים העולים בדוח זה ובנושא זה, מומלץ לעיין ולפעול בהתאם להמלצות מערך הסייבר הלאומי - הגנת סייבר ברשויות – מערכת יוב"ל: https://www.265.org.il/database/%d7%94%d7%92%d7%a0%d7%aa-%d7%a1%d7%99%d7%99%d7%91%d7%a8-%d7%9c%d7%a8%d7%a9%d7%95%d7%aa-/%d7%94%d7%9e%d7%a7%d7%95%d7%9e%d7%99%d7%aa

8. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות

תקנה 5 לתקנות אבטחת המידע קובעת כי יש לבצע מיפוי מערכות המאגר:

(א) 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.

(ב) המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן – סקר סיכונים); בעל מאגר

המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו.

(ה) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי כאמור בתקנת משנה (א), במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה וכן רשאי לקיים את החובות הקבועות בתקנות משנה (ג) ו-(ד) בסקר סיכונים או במבדק חדירות, לפי העניין, אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה.

באשר לביקורות תקופתיות, תקנה 16 קובעת:

(א)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר אחראי לכך שתיערך, אחת ל-24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.

(ב)

בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

(ג)

בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

(ד)

בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת עריכת סקר סיכונים שמתקיים בו האמור בתקנת משנה (ב).

(ה)

ארגון שהוא בעל כמה מאגרי מידע, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת ביקורת אחת לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.

ממצאים

במועצה אין מדיניות סדורה באשר למיפוי, סקר סיכונים ובקרה. במועצה לא בוצע מיפוי של מערכות המאגר כנדרש, לא בוצעו סקר סיכונים מקיף ומפורט בתחום אבטחת המידע, כמעט ולא בוצעו מבדקי חדירה ולא מבוצעות בקרות תקופתיות. יוער, כי באמצעות ממונה אבטחת המידע שהינו גורם מקצועי ומבין המצב יותר טוב מזה שהיה בבדיקת הביקורת בשנת 2015, אך התקציב העומד לרשותו לא מאפשר לו להמשיך לרמה הנדרשת.

המלצות

על מנת שהמועצה תעמוד בתקנות אבטחת המידע ותהיה מוכנה לטיפול בחולשות ובסיכונים במערכות המחשוב והמידע, עליה לבצע סקרי סיכונים, מבדקי חדירה וביקורות תקופתיות.

הביקורת ממליצה למועצה לקבוע עקרונות ומתודולוגיה לניהול סיכונים בתחום אבטחת המידע, לנהל באופן שוטף את הסיכונים, לבצע מבדקי חדירה בהתאם לדין ולצורך (לפי רמת המאגר), לקבוע נהלים בתחום, לקבוע סמכויות ותחומי אחריות ולבצע בקרות.

ייתכן וראוי לפעול לגבי כלל המאגרים כמו שיש לפעול בעניין המאגרים שחלה עליהם רמת אבטחה גבוהה, שכן בכל המאגרים תיתכן פגיעה בפעילות השוטפת של המועצה וברמת השירות, וזאת מעבר לפגיעה בפרטיות.

דוג' לתרשים בנושא ממשרד ראש הממשלה - שלבי תהליך ניהול סיכונים באגף מערכות מידע:

9. תקצוב אבטחת מידע

נושא חוזר מדוח 2015 (כליקוי שלא תוקן וכמעט כלשונו).

תקנה 3(6) לתקנות אבטחת המידע קובעת כי "בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו".

ביום 15.02.2015 התקבלה החלטת ממשלה מספר 2443 בנושא: קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר.

החלטה זו באה בהמשך להחלטת הממשלה מספר 3611 מיום 07.08.2011 בנושא "קידום היכולת הלאומית במרחב הקיברנטי", בהתאם לתפיסה הלאומית להגנת הסייבר, לטובת

העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר במדינת ישראל ובכפוף להחלטת הממשלה מספר 2118 מיום 22.10.2014.

ההחלטה עסקה במספר נושאים: האסדרה הלאומית בהגנת הסייבר, תחום ההובלה הממשלתית בהגנת הסייבר, עבודת מטה שבמסגרתה ייבחן האם ובאיזה אופן תוחל החלטה זו על משרד הביטחון ויחידותיו, פעילות בינלאומית של הרשות הלאומית להגנת הסייבר.

במסגרת ההחלטה ישנן מספר התייחסויות תקציביות. לגבי הקצאת תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של משרדי הממשלה, נקבע:

"א. המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, יסדירו את מבנה התקציב השנתי של משרדם כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

ב. מנכ"ל משרד ממשלתי או מנהל יחידת הסמך, לפי העניין, יוכל בנסיבות מיוחדות לאשר הפחתה מהאמור בהחלטה מפורטת ומנומקת שתדווח לוועדת ההיגוי הממשלתית כמפורט בנספח ח' להחלטה זו, ובלבד שלפחות 6% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

ג. בתום שנתיים ממועד החלטה זו, ועדת ההיגוי הממשלתית תבחן את הצורך בהעלאת אחוז התקציב הייעודי להגנת הסייבר".

בזמן הביקורת הקודמת, נוהל המסגרת במשרד רוה"מ קבע, כי שיעור תקציב פעילות אבטחת המידע, צריך להיות לפחות 5% מהתקציב השנתי לרכישת חומרה, תוכנה ותשתיות, להעסקת יועצים ולביצוע סקרים. הביקורת לא באה לקבוע איזה אחוז נכון לקבוע במועצה, אך נוהל המסגרת יכול לתת כיוון.

ממצאים

הביקורת העלתה, כי במועצה לא הוצגו להנהלה ולא נקבעו תקציבים ייעודיים לאבטחת מידע, אלא הם נכללים בסך תקצוב המחשוב.

המלצות

לדעת הביקורת, ראוי כי המועצה תתקצב את אבטחת המידע בסעיף תקציב ייעודי כחלק יחסי מתקציב המחשוב ומערכות המידע. מומלץ לבחון את גובה תקצוב לאור ממצאי הביקורת ולקבוע אותו בהתאם לייעוץ שיינתן למועצה בנושא.

10. הדרכה וקיום אבטחת מידע אצל עובדים

נושא חוזר מדוח 2015 (כליקוי שלא תוקן וכמעט כלשונו).

תקנה 7 לתקנות אבטחת המידע קובעת:

(א)

לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו הנוגע בדבר, כאמור בתקנה 8.

(ב)

בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם, יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע על אודות חובותיהם לפי החוק ונוהל האבטחה.

(ג)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש – סמוך ככל האפשר למועד תחילת הסמכתו.

הדרכת משתמשים ועובדים, חדשים, קיימים ועוזבים, בנושאי אבטחת מידע, נועדה להבטיח כי עובדי הארגון יהיו ערים לקיומם של גורמי סיכון בשימוש במערכות המידע ולחשיבות הפעולות לאבטחת המידע בארגון.

נושא אבטחת המידע לא תמיד מצוי על סדר יומם של המשתמשים, ונדרשת יוזמה, הדרכה והטמעה על מנת להגביר את המודעות וממילא את אבטחת המידע.

בנוהל המסגרת, נקבעו פעולות הדרכה והסברה בתחומי אבטחת המידע ובין היתר: הטמעת עקרונות וכללי אבטחת המידע למשתמשים בכל הממשקים; הקצאת תקציב הולם לפעילות ההדרכה; אחריות ממונה אבטחת המידע לייזום פעילויות הדרכה והסברה בקרב כל העובדים בארגון; הדרכת העובדים בעניין שמירת הסיסמאות; תגובה בעת חשד לחשיפת סיסמה; הדרכה למשתמשים בנושא נוהלי אבטחה ובנושא השימוש הנכון באפשרות לעיבוד מידע, כדי למזער סיכוני אבטחה אפשריים; סוגיית הדרכת עובדים טרם מתן הרשאות וגישה למחשוב; הדרכה למשתמשים חדשים וריענון לוותיקים; פעולות להגברת מודעות המשתמשים; תדרוך לגבי דיווח בעת התרחשות

אירועים חריגים שעלולים להשפיע על אבטחת המידע ; הסקת מסקנות מאירועים בתחום אבטחת המידע.

ממצאים

המועצה לא נוקטת אמצעים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר. עובדים חדשים או כל גורם שמקבל גישה למאגר או למערכות המאגרים, אינם עוברים תהליך מיון ולא נבדקת התאמתם לקבלת הגישה למאגרי המידע.

אגף הסייבר במשרד הפנים קיים הדרכות בנושא אבטחת מידע באמצעים מקוונים לעובדי רשויות, אך המועצה לא תיאמה הדרכה כזו.

המועצה לא מקיימת פעולות הדרכה והסברה בתחום אבטחת המידע לעובדים. מבדיקת הביקורת עולה, כי לא התבצעו פעולות הדרכה המתאימות לעת סיום יחסי עבודה של עובדים.

המלצות

על המועצה לתת גישה למידע המצוי במאגריה או לשנות היקף הרשאה שניתנה, רק לאחר שתנקוט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה מתאים לקבלת גישה למידע המצוי במאגר.

על המועצה לקיים פעולות הדרכה והסברה בתחום אבטחת המידע בדומה לדרישות המפורטות בנוהל המסגרת או לפי נוהל מתאים שתקבע לנכון,[29] וזאת עד שתצאנה הנחיות מסודרות ממשרד הפנים, משרד המשפטים או מגורמי רגולציה אחרים.

על המועצה לגבש תוכנית הדרכה כוללת להגברת מודעות העובדים בכל ההיבטים הנוגעים לאבטחת מידע ובכלל זה הדרכה בנהלי המועצה בתחום זה וריענון מעת לעת כולל תיעוד לגבי כל עובד.

מומלץ שהמועצה תנקוט פעולות להגברת המודעות, החשיבות, הסיכונים והאיומים בתחום אבטחת המידע.

11. חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת

בעניין אבטחת תקשורת, תקנה 14 לתקנות אבטחת המידע קובעת:

(א)

בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

(ב)

העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

(ג)

29 מלבד הדרכה כללית, ממונה אבטחת המידע הציע הדרכה לבכירים, מנהלים ועובדים.

במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.

ממצאים

מדיניות הגלישה מתירנית ביותר. אין חסימה לקטגוריות מסוכנות.

משתמשי הקצה יכולים להתקין להתקין תוכנות ולבצע מגוון שינויים בהגדרות כמעט ללא פיקוח.

נושא חומת האש ואנטי וירוס נבדק בשנת 2015. אבטחת המידע הלוגית מתקיימת, בין היתר, באמצעות "חומת אש" (FireWall), ואנטי וירוס של eset.

בזמנו, במהלך הביקורת התברר כי לא כל תוכנות האנטי וירוס מעודכנות. המצב תוקן באופן מיידי. ממונה אבטחת המידע מסר, כי כיום המצב תקין והוא דואג לעדכונים כנדרש.

הביקורת לא הצליחה לוודא הגנה ראויה לתחנות הקצה.

אין התייחסות מיוחדת להעברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט ולגבי גישה מרחוק (מנהל מערכות המידע יכול לגשת בקלות לכל מחשב ללא כל יידוע משתמש הקצה).

מנהל מערכות המידע, מסר כי הוא דואג לעדכן את מערכות התוכנה. בתחום החומרה היה רוצה לעדכן יותר, אך מדובר בנושא תלוי תקציב.

אין הגנה מיוחדת על הטלפונים הניידים במועצה.

המלצות

יש להמשיך לעדכן ולעקוב באופן שוטף אחר רמת חומת האש (FireWall) והאנטי וירוס במועצה ובכלל זה דאגה מתמדת להתקנת עדכונים מיד עם פרסומם.

מוצע להיוועץ בגורם חיצוני באשר למדיניות הגלישה, מרחב השימוש של משתמש הקצה, לגבי העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, לגבי מאגרים שניתן לגשת אליהם מרחוק, שימוש בשיטות הצפנה מקובלות, בחינת מוצרי האבטחה הקיימים ובכלל זה בחינת צורך בשדרוג והוספת כלי אבטחה וכו'.

על מנת לנטרל מראש חולשות ופגיעות, על המועצה לעדכן באופן שוטף את מערכות המאגרים, התוכנה והחומרה בהתאם להנחיות היצרן ולצורך.
מומלץ לבחון היטב את ההגנה הארגונית גם ברמה המחלקתית ושל תחנות הקצה ולתקן את הדרוש תיקון כולל מידור נדרש בין תחנות.

מומלץ לבצע הגנת אבטחת מידע לטלפונים הניידים במועצה.

מומלץ להיוועץ עם גורם מקצועי לצורך הגברת האבטחה באופן כללי ובהקשר דנן גם לאבטחת גישה מרחוק.

12. שמירה, גיבוי ושחזור של נתוני אבטחה

תקנה 17 לתקנות אבטחת המידע עוסקת בשמירת נתוני אבטחה ותקנה 18 עוסקת בנושא גיבוי ושחזור של נתוני אבטחה. בין היתר, התקנות קובעות, כי יש לקבוע נהלים לביצוע גיבוי ולהבטחת שחזור הנתונים וכן יש לבצע הליכי שחזור מידע.
בהקשר לדברים אלו ובכלל, ראוי לציין כי על רשות מקומית להיערך באמצעות תוכנית סדורה למצב של התאוששות מאסון סייבר כמו פריצה למאגרי המידע של הרשות, השתלטות על מאגרים, אירועי כופרה ועוד.
לפי המתווה להקמה ולהפעלה של יחידות לניהול מערכות מידע ברשויות המקומיות שהכין משרד הפנים בשנת 2019, על הרשות המקומית להכין תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית לפעולת יחידת מערכות המידע ובין היתר בנושא של פיתוח ושדרוג תשתיות קיימות, רכש ציוד, והתקשרות עם גורמים במיקור חוץ לעמידה ביעדי התוכנית.

עוד נקבע במתווה משרד הפנים שיש ליישם את תוכנית העבודה האסטרטגית לאחר שימופה המצב הקיים ברשות כמו שרתים, תשתיות תקשורת, רשתות, מערכות מידע וכלים דיגיטליים, וכן השירותים הדיגיטליים, אבטחת המידע, ניהול מאגרי המידע וההגנה על הפרטיות. נוסף על אלו, יש לבצע איתור של צורכיהן הטכנולוגיים של היחידות השונות ברשות כדי לברר מה נדרש להן, מהבחינה הטכנולוגית, על מנת שיוכלו ליישם את תוכניות העבודה שלהן.

המועצה, גם לפי תורת ההגנה, אחראית להכנת תוכנית עבודה רב-שנתית להגנה ולהתאוששות מאירועי סייבר. בין היתר, יש למפות את הסיכונים, לגבש מענה הגנתי, להכין וליישם תוכנית להפחתת הסיכונים.

ממצאים

מנהל מערכות המידע מסר, כי הוא ערוך להתמודדות עם אירועי סייבר ככל שהתקציב מאפשר. למועצה אין תוכנית סדורה ומאושרת להתמודדות עם אירועי סייבר.

למועצה אין נוהל גיבויים כנדרש. מנהל מערכות המידע דואג לביצוע גיבויים, אך הוא לא מלא (כך למשל נמסר ממשתמשים במחשבים ניידים שלא ערכו גיבוי שוטף).

המלצות

ככלל, לאורך דוח זה עולה הצורך של המועצה להכין תוכנית עבודה כוללת ואסטרטגית שתשמש בסיס לתוכניות עבודה שנתיות. בכלל זה תוכנית להתאוששות מאסון.

על המועצה לפעול לפי מתווה משרד הפנים. מומלץ למועצה לפעול בהתאם לתורת ההגנה, ובכדי לגבש תוכנית עבודה לשיפור ההיערכות לעניין ההגנה מפני אירועי סייבר, להגדיר על מה המועצה נדרשת להגן, מהי רמת ההגנה הנדרשת, ובאילו תחומים עליה להשתפר כדי להגיע לרמה זו.

על המועצה להיערך באופן מסודר תוך הכנת תוכנית ראויה למצב של התאוששות מאסון. תוכנית כזו תסייע למועצה להמשיך לתפקד כראוי ולהתמודד טוב יותר עם אירועי סייבר כגון גניבת מידע, פריצה למאגרים, מחיקת מידע ועוד.

מומלץ למועצה לבחון היטב את הצורך ובהתאם לכך להיערך גם תקציבית.

13. רישוי תוכנות

ממצאים

בשונה מהמצב המתואר בדוח 2015 בו היו מספר עמדות ללא רשיונות או עם רשיונות לא מעודכנים ולא נערך מעקב (כבר אז המצב תוקן), מממונה אבטחת המידע נמסר, כי ממשיכים להקפיד על כך ומתבצע מעקב.

המלצות

הביקורת ממליצה, כי מעת רכישה והתקנה יוודא נושא הרישוי ויתועד באופן מסודר, ממוחשב וברור.

מובן, שמנהל אבטחת מידע וקיום נהלים וגורמי סיוע אחרים, אשר נידונים בדוח זה יסייעו וידאגו גם הם לתקינות בתחום הרישוי.

14. אבטחה פיזית וסביבתית

תקנות הגנת הפרטיות שמות דגש גם לאבטחה הפיזית של המאגרים. להלן תקנה 6:

(א) בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

(ב) בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.

ממצאים

יצוין, כי הביקורת העלתה ליקויים בנושא זה בדוח 2015. אומנם המצב טוב יותר (פחות גישה פיסית), אך עדיין לא במצב שפיר לפי התקנות.

הביקורת בחנה את האבטחה הפיזית והסביבתית של מקום ארונות התקשורת והשרתים בהם נשמרים המאגרים (ישנם מאגרים אחרים שנשמרים בענן).

נמצא כי הסביבה הפיזית בה נשמרים ארון התקשורת והשרתים של המועצה אינם אינה הולמת ואינה עומדת בדרישות התקנות.

דוג' לליקויים ממוקדים: בחדר השרתים לא קים תיעוד הנכנסים ואת הנעשה בחדר; אין הרשאות כניסה לחדר; לא קיים חיישן טמפרטורה; היעדר מערכת כיבוי אש; היעדר התראות לאחראי ברשות בעת אירוע הדורש טיפול מיידי, כגון כניסת בלתי מורשים לחדר השרתים, שרפה, תקלות טכניות, תקלות חשמל, הפסקת תקשורת וכו'; אין התייחסות ביטחונית מיוחדת.

המלצות

על המועצה לקיים את הוראות התקנות בעניין האבטחה הפיזית והסביבתית.

בשלב ראשון ומיידי, רצוי להתקין קודן, מצלמות אבטחה ודלת מתאימה. בהמשך ראוי להיוועץ בגורם מקצועי ולפעול בהתאם.

15. ניהול הרשאות גישה וזיהוי ואימות

תקנות 8 ו- 9 לתקנות אבטחת המידע מתייחסות לנושא הרשאות גישה וזיהוי ואימות. להלן ציטוט מהתקנות:

8. (א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).

9. (א) בעל מאגר מידע ינקוט אמצעים מקובלים בנסיבות העינין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה –

(1) אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה;

(2) ייקבעו בנוהל האבטחה גם הוראות לעניין תקנת משנה (א), ובכללן בנושאים אלה:

(א) אופן הזיהוי; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על שישה חודשים;

(ב) ניתוק אוטומטי לאחר פרק זמן של אי-פעילות;

(ג) אופן הטיפול בתקלות הקשורות באימות זהות.

(ג) בעל מאגר מידע ידאג לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

ממצאים

יצוין כי בדוח 2015, הועלו ליקויים בנושא ניהול ההרשאות וסיסמאות.

המועצה לא ביצעה מיפוי הרשאות, ואינה מקפידה על נהלי הרשאות, תיקוף הרשאות, זיהוי ואימות כנדרש בתקנות. לא קיים ניהול רישום מעודכן של ההרשאות הגישה למאגרי מידע שניתנו לעובדים.

נמצא כי לא קיים נוהל / טופס בקשת הרשאות הכולל את הפרטים הנדרשים ; לא בוצע מיפוי לסוגי ההרשאות הנדרשות.

במועצה אין הזדהות חזקה לגישה מרחוק למשתמשי הקצה וגם מנהל מערכות המידע ועובדיו נכנסים למחשבים ולמערכות המידע באמצעות גישה מרחוק פשוטה ואף ללא צורך בסיסמאות חד פעמיות.

מחדלים אלו חושפים את המועצה לסיכונים הכוללים חשיפה לא מורשית למידע.

המלצות

על המועצה לפעול בהתאם לתקנות. כך למשל, יש לקבוע נוהל כאמור לעיל ובו התייחסות נדרשת לתחום ההרשאות ; לקבוע הרשאות גישה למאגר לכל עובד במידה הנדרשת לו לצורך ביצוע תפקידו ולא יותר מזה ; יש לבצע מיפוי ורשימת הרשאות ולעדכנה לפי הצורך ובעת שינוי ; יש לבטל הרשאות למי שסיים תפקידו – מייד עם סיום התפקיד.

מומלץ לבחון ולקבוע אופן אבטחת גישה מרחוק המתאים לרמת המאגרים.

בד"כ מקובל להמליץ שהזיהוי והאימות יתבססו על אמצעי פיזי הנתון לשליטתו הבלעדית של מורשה הגישה (ביומטרי, כרטיס חכם או Token הנשלח כהודעת SMS לטלפון הנייד). בזיהוי מבוסס שם משתמש וסיסמה יש לקבוע את חוזקה, מספר ניסיונות שגויים ותדירות החלפה. כמו כן, נדרש ניתוק אוטומטי לאחר פרק זמן של אי-פעילות. המלצה זו כפופה להגדרות והתאמות מקצועיות.

מעת לעת ובהתאם לצורך, יש לבחון ולעדכן את רמת ההרשאות לשם צמצום הסיכונים ומניעת נוזקות.

16. חיבור התקנים

תקנה 12 לתקנות אבטחת המידע קובעת :

"בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה ; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים

המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד".

ממצאים

במועצה אין הגבלה מספקת בחיבור למערכות שלה באמצעות חיצוניים (כך, מלבד שימוש בהתקנים ניידים קטנים עם USB, ניתן להתחבר ישירות לרשת המועצה כמו שנעשה לעיתים באמצעות מחשבים ניידים בין אם בידי עובדי המועצה ובין אם בידי נותני שירותים או מבקרים). אי הגבלה זו חושפת את המועצה לסיכוני אבטחת מידע. בנוסף לכך, לא בוצע ניתוח של הנושא כנדרש בתקנה 12 לתקנות אבטחת המידע.

המלצות

על המועצה לעמוד בתקנה 12 לגבי חיבור התקנים.

מומלץ להייעוץ בגורם מקצועי.

17. בקרה ותיעוד גישה

תקנה 10 לתקנות אבטחת המידע קובעת כי במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או גבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע. לשון התקנה:

(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

(ב) מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

(ג) בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

(ד) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

(ה) בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

ממצאים

המועצה לא מיפתה את נושא התיעוד האוטומטי עבור כל מאגר ולא נקבע נוהל בדיקה לנתוני התיעוד.

מממונה אבטחת המידע נמסר, כי יש מספר מאגרים עם בקרה והגבלת גישה (כגון מאגרים בחברה לאוטומציה, בר טכנולוגיות (ועדה מקומית לתכנון ולבניה) ומערכת מימד – רישום נתוני משרד הפנים עבור התושבים).

לגבי שאר המאגרים, הביקורת מעירה, כי ללא בדיקת התיעוד לא ניתן לדעת האם גורם בלתי מורשה ניגש למאגרים עם מידע רגיש. הדברים מקבלים משנה תוקף במאגרים עם "משתתף משותף" וכך אין אפשרות לדעת על זהות מבצעי הפעולות.

אין ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות של גורמים בלתי מורשים.

המלצות

על המועצה להפעיל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע בהתאם למפורט בתקנה.

מומלץ להגדיר את מנגנון התיעוד ולערוך שינויים ועדכונים בהתאם לצורך.

יש לבצע ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות של גורמים בלתי מורשים.

18. תיעוד של אירועי אבטחה

תקנה 11 לתקנות אבטחת המידע העוסקת בתיעוד אירועי אבטחה קובעת:

(א) בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן – אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

(ב) בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל

האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.

(ד) אירע אירוע אבטחה חמור –

(1) יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע;

(2) רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

ממצאים

למועצה אין נהלים לאיתור, תגובה ותרגול של אירועי אבטחת מידע, אין מדיניות בנושא ואין תיעוד. עד מינוי ממונה אבטחת מידע, לא בוצעה בדיקה מסודרת של מרבית אירועי אבטחת המידע. גם כעת, התקציב לא מאפשר ניטור רציף ברמה גבוהה, ולא ניתן לדעת בוודאות שלא היו אירועים כאלה. היה ניסיון לפגיעה במחשבי הוועדה לתכנון ולבניה שהסתיים מהר מאד בזכות ממונה אבטחת המידע ולפי אנשי המחשוב לא התפתח לכדי אירוע.

פורום הנהלה או דרג ניהולי כלשהו לא מקיים דיונים באירועי אבטחה, אין תרגול ואין צוות מקצועי למענה מקצועי לסיכוני ואירועי סייבר.

המלצות

על המועצה לפעול באופן סדור בהתאם לתקנה 11 לתקנות אבטחת המידע בנושא תיעוד אירועי אבטחת מידע, מומלץ לקבוע מדיניות, ליישם טכנולוגיה מתאימה לניטור ואיתור אירועים חריגים ותגובה להם, לקבוע נהלים לאיתור ותגובה לאירועי אבטחת מידע וכן לתרגל.

מומלץ למנות צוות המשכיות והתאוששות מאסון, לקבוע סדר ומדרג פעולות תגובה בהתאם לאירוע האבטחה ולהתפתחותו ולעדכנו בהתאם לצורך.

כעולה מדוח זה, ובהקשר לנדון, מומלץ להיערך מבעוד מועד לאירועי אבטחה שונים ומגוונים ובכלל זה לקבוע מנגנון קבלת התראות, לבצע הדרכות וכו'.

19. עיר חכמה

בהחלטת ממשלה מספר 2733 של ממשלת ישראל מיום 11.06.2017 אושרה התוכנית הדיגיטלית הלאומית, קידום המיזם הלאומי "ישראל דיגיטלית".

בהגדרת חזון המיזם הלאומי ומטרותיו, נכתב ש"ישראל תמנף את ההזדמנות הטמונה במהפכה הדיגיטלית ובהתקדמות טכנולוגיות המידע והתקשורת כדי לאפשר צמצום

פערים חברתיים וגיאוגרפיים, צמיחה כלכלית מואצת, וקידום ממשל חכם וידידותי לאזרח, ומוביל עולמי בתחום הממשל הדיגיטלי״.

במסגרת ההחלטה, הוטל על מספר מנכל״י משרדי ממשלה לגבש תוכנית לקידום תחום הערים החכמות בישראל, שבין מטרותיה צמצום פערים וחיזוק הפריפריה הגאוגרפית והחברתית, ולפעול ליישומה.

כיום אין הגדרה מוסכמת ל״עיר חכמה״ ורשויות יוצקות תוכן להגדרה. בכל אופן, הכוונה היא בשימוש רחב בטכנולוגיות מידע ותקשורת בעולמות התוכן השונים של הרשויות, וזאת על מנת להגביר שירותיות, יעילות תפקודית, רווחה, איכות חיים, בטיחות וביטחון כלכלה ועוד.

ברור כי מדובר ברשויות שפועלות עם מגוון כלים טכנולוגיים שמחייבים מתן דגש לאבטחת מידע ושמירת הפרטיות.

תרשים מתוך מדריך הגנת הפרטיות לעיר החכמה:[30]

[30] https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

הרשות להגנת הפרטיות פרסמה "מדריך להגנת הפרטיות בעיר חכמה".[31]

ממצאים

בשלב זה, המועצה לא החליטה על מעבר ל"עיר חכמה" לפי כל הגדרה שהיא ולא פועלת להטמעת טכנולוגיות מתקדמות חדשות לטובת התושבים.

המלצות

בכל הקשור ל"עיר חכמה" ולהטמעת טכנולוגיות חדשות, מומלץ למועצה לגבש מסקנות והחלטות רק לאחר היוועצות בגורמי מקצוע, לימוד הצורך והכרת ההזדמנויות והסיכונים.

20. מיקור חוץ

חלק ממאגרי המידע של המועצה מוחזקים על יד גורמים חיצוניים במיקור חוץ.

תקנה 15 לתקנות אבטחת המידע קובעת:

(א) 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 ההתקשרות;

(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

31 מסמך מעודכן משנת 2020
https://www.gov.il/BlobFolder/news/smart_city_guide_2020/he/smart%20city%20guide%202020.pdf

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).

(ב) ארגון שהוא בעל כמה מאגרי מידע, המתקשר עם גורם חיצוני לצורך מתן שירות הכרוך בגישה אליהם בידי הגורם החיצוני, רשאי לקיים את הוראות תקנת משנה (א)(2) בהסכם אחד לעניין כל מאגרי המידע ובלבד שהם באותה רמת אבטחה.

(ג) תקנה זו לא תחול על התקשרות של בעל מאגר עם יחיד.

בדיקה טרם יציאה למיקור חוץ

בהתאם לתקנות והנחיות הרשות להגנת הפרטיות נדרש לבצע בדיקה טרם הוצאת המאגרים למיקור חוץ:

א. טרם ביצוע התקשרות עם גורם חיצוני, לבחון את סיכוני אבטחת המידע הכרוכים התקשרות – תקנה 15 (א) (1)

ב. להכין מסמך המפרט מדוע השירות מתבצע במיקור חוץ (הנחיה 2/2011)

הסכמים עם מחזיקי מאגרים במיקור חוץ

על פי תקנה 15 נדרש לחתום על הסכם עם מחזיקי מאגרים חיצוניים, ואל ההסכם לכלול את הסעיפים הבאים:

א. סעיף שמחייב את מחזיק המאגר לעמוד בחוק הגנת הפרטיות והתקנות שלה.
ב. תיאור של המידע שמנוהל במערכת.
ג. אופן השבת המידע/השמדתו בסוף ההתקשרות (מה עושים עם המידע לאחר תום ההתקשרות).
ד. חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.
ה. חובתו של גורם החיצוני לדווח, אחת לשנה לפחות, על אופן ביצוע חובותיו לפי התקנות.

כמו כן, על פי הנחיות רשם מאגרי המידע 2/2011 נדרש לכלול את הנושאים הבאים בהסכם:

א. הגדרה ברורה של מטרות שימוש מותרות על ידי הקבלן ומורשי גישה מטעמו.
ב. נדרשת התחייבות הקבלן שהוא מינה ממונה אבטחת מידע אצלו.
ג. נדרש סעיף שמירה על זכויות המזמין לבצע ביקורת באתר הקבלן ולפקח על פעילות (לרבות ביקורת פתע).
ד. נדרש לקבוע קביעת פרק הזמן בו נשמר המידע אצל הקבלן ומחיקת מידע בתום ההתקשרות.

מעבר להכללת התחייבויות הקבלן, על המועצה לבצע פעולות כדי לוודא שהספק עומד בהתחייבויותיו לאבטח את המידע.

ממצאים

נמצא כי במועצה לא נערכה עבודה מקדימה הקשורה לבחינת ההשלכות של שימוש במיקור חוץ לניהול מאגרים עם מאפיינים של הגנת הפרטיות.

נמצא כי המועצה אינה מקפידה על הסכמים עם ספקי שירותי מערכות מידע, אשר מחייב אותם לשמור על הגנת הפרטיות בהתאם לתקנות.

עוד עולה, כי גם כאשר יש בהסכמים סעיפים המחייבים את הספקים במיקור חוץ לאבטח את המידע, המועצה לא נקטה צעדים כדי לוודא או לבקר את עמידת הספק בהתחייבות.

במועצה אין דרישה, פיקוח או בקרה למילוי חובות הספקים כמחזיקי מאגרי מידע. יודגש, כי כאמור, בהתאם לסעיף 17א לחוק הגנת הפרטיות, מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר; מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

מהחברה לאוטומציה נמסר, כי מדיניות האבטחה שלהם מסודרת ומעוגנת בנהלי אבטחה מסודרים ומתוקננים תחת תקן אבטחת מידע מתקדם ואף העבירה לביקורת מידע בנושא.

בתשובה לשאלת הביקורת, השיבה החברה לאוטומציה כי: "החברה לאוטומציה הינה ספק השירותים למועצה האזורית לכיש, ובפוזיציה זו היא מחויבת לעמוד בדרישות האבטחה של הרשות, ולא להיפך. ובכל זאת, החברה לאוטומציה ממליצה ללקוחותיה, ובהם ספציפית גם בפעילות מול לכיש, לקיים רמת אבטחת מידע הכוללת הגנה על כלל תחנות הקצה, שמירה על נהלי סיסמאות, הגנת וירוסים, בקרת גלישה ומיילים וכד'.

החברה לאוטומציה מפעילה את מערכות המחשוב כאשר נהלים אלה מובנים, והלקוח נדרש להחליף סיסמאות מעת לעת, מסכי המערכת ננעלים לאחר זמן של חוסר שימוש, הלקוח קובע את מרחבי הכתובות מהם ניתן להפעיל את מערכות המחשוב שלו וכד'".

בעניין שאלה על מאגרי המידע, מהחברה לאוטומציה נמסר, כי היא מוגדרת כ"מחזיקת המאגר" והמועצה היא "בעלת המאגר".

הביקורת הפנתה שאלות גם לחברת מילגם המספקת שירותי גביה. להלן חלק מתשובותיה:

"החברה אינה מספקת שירותי מחשוב למועצה. שירותי המחשוב ניתנים למועצה ע"י החברה לאוטומציה. מילגם כן מאפשרת לעובדיה המוצבים במועצה אפשרות שימוש בתוכנה פנימית של מילגם לביצוע פעולות אכיפה כלפי חייבים וכן מערכת המייל. מערכות השייכות למילגם מנוהלות כולן בחוות השרתים של חברת מילגם. עובדי החברה כפופים להנחיות אבטחת המידע של החברה. החברה מנהלת את שכבות האבטחה השונות באמצעות עמידה בתקן מחמיר של אבטחת מידע, כלים טכנולוגיים להגנה מאגרי המידע, הנחיות ומודעות לעובדים ועוד.

בוצעה התעדה מלאה למערכת ניהול אבטחת המידע על ידי מכון התקנים הישראלי אשר מוכיחה שהארגון נוקט באמצעים המתאימים בכדי לממש את מחויבותו לשמירה על המידע ולנהלו בצורה יעילה.... כל מאגרי המידע שמנוהלים בחוות השרתים של מילגם מנוהלים עם דגש נרחב בתחום אבטחת המידע".

החברה השיבה תשובות שליליות לשאלות הביקורת:

האם המועצה הציבה לחברתכם דרישות בתחום אבטחת המידע; האם בהסכמים עם המועצה יש דרישה לעמוד בתקני אבטחת מידע ופרטיות; האם המועצה בודקת מולכם עמידה בהסכמים בנושא זה?

לשאלת הביקורת, בקשר למאגרי המידע, החברה השיבה שהיא אינה בעלת המאגר ולכן לא צריכה לרושמו.

גם בקשר למוקד המועצה הביקורת לא מצאה מדיניות סדורה, התייחסות בהסכמים ואכיפה כאמור.

המלצות

מומלץ למועצה לקבוע מדיניות בתחום מיקור החוץ, וכמובן עליה לעמוד בכללים.

מומלץ כי המועצה תבחן את סיכוני אבטחת המידע הכרוכים בהתקשרויות.

על המועצה לקבוע בהסכמים עם הגורמים החיצוניים את כל הכללים הנדרשים בהתאם לתקנה 15 ולצורך, ובכלל זה: קביעת מערכות המאגר אליהן רשאי לגשת הספק, סוג הפעולות שהספק רשאי לעשות, המידע שהספק רשאי לעבד, מטרות השימוש, גיבויים, דרך העברת מידע במהלך ההתקשרות, דרך השבת והעברת המידע לידי המועצה בסיום ההתקשרות, כללי אבטחת מידע קונקרטיים, תצהירי סודיות, ועוד כמפורט לעיל.

מלבד האמור לעיל, על המועצה לפרט בנהלים את הנדרש בהתאם לתקנות, ולנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות כנדרש.

כמו כן, מומלץ לפנות לספקי מיקור החוץ ולדרוש מהם הצהרות ואסמכתאות לעמידה בתקנות, לרבות ביצוע מבדקי חדירה, סקרי אבטחה ותעודות תקני אבטחה ולבקרם בהתאם לרמה הנדרשת מכל אחד מהם.

21. מינוי ממונה אבטחת מידע

על פי סעיף 17ב לחוק הגנת הפרטיות, המועצה מחויבת במינוי ממונה על אבטחת מידע:

17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(2) גוף ציבורי כהגדרתו בסעיף 23;

(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

(ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

(ג) *לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.*

כל "גוף ציבורי" כהגדרתו בסעיף 23 לחוק הגנת הפרטיות ובכלל זה הרשות המקומית, שהינה חלק מהגופים המנויים בסעיף זה, חייב, לפי סעיף 17ב לחוק הגנת הפרטיות, במינוי אדם בעל הכשרה מתאימה שיהיה ממונה ואחראי על אבטחת המידע במאגרים המוחזקים ברשותו, באשר להגנה על שלמות המידע, הגנה על המידע מפני חשיפה, שימוש או העתקה.

תקנה 3 לתקנות אבטחת מידע קובעת כי:

חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה:

(1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחת הכפוף ישירות למנהל המאגר;

(2) הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר;

(3) הממונה יכין תוכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;

(4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;

(5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות בפסקאות (2) ו-(3), לשם ביצוע תקנות אלה, יגדירן בצורה ברורה;

(6) בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.

בהתאם לנוהל שיצא ממשרד ראש הממשלה (והוזכר בדוח הביקורת במועצה בשנת 2015 (להלן: "דוח 2015"), תפקידיו העיקריים של ממונה אבטחת מידע:

א. פיתוח, עדכון, הדרכה, הטמעה, הפצה ובדיקת היישום של נוהלי אבטחת מידע בכל הדרגים ובכל המערכות.

ב. מתן ייעוץ בנושאי אבטחה ובקרה בעת פיתוח יישומים חדשים וקבלת מערכות מידע חדשות.

ג. בדיקת יישומים קיימים ומתן ייעוץ לשיפור הבקרות בהם.

ד. טיפול שוטף בהרחבת המודעות לסוגיות אבטחת מידע בדרגים השונים.

ה. הכנת תוכנית פעילות שנתית בנושאי אבטחת מידע, במסגרת ועדת היגוי למחשוב ועמידה ביעדים שהוצבו.

ו. דיווחים לוועדת היגוי למחשוב.

ז. סיוע במיפוי וסיווג של מאגרי המידע השונים.

ח. אחזקת הרישום המעודכן של כל היישומים וסיווגם.

ט. חברות בוועדת ענ"א (עיבוד נתונים אלקטרוני).

י. תיאום עם גורמי הביקורת וביטחון המשרד.

יא. מיפוי ההרשאות, כולל עדכון שוטף.

יב. הגדרת פעילויות חריגות.

יג. מעורבות בהתקשרות עם גורמי חוץ רלוונטיים ומתן הנחיות אבטחת מידע על פי הצורך.

יד. פיקוח על שירותי ספקים רלוונטיים.

טו. יעוץ בעת חתימת חוזים רלוונטיים.

טז. ריכוז כל סיכומי אירועי ה"וירוסים", תקלות וניסיונות פריצה במשרד.

יז. השתתפות בהכנת תוכנית התאוששות מאסון והמשכיות עסקית.

יח. ייזום בדיקות תקופתיות במחשבים אישיים.

יט. ייזום בדיקות תקופתיות של רשת החשמל וציוד מיגון למערכות מחשוב במשרד.

כ. ייזום תקופתי של בדיקות סיכוני האש ומערכת המניעה, ע"י מומחים.

כא. קשר עם רשם מאגרי המידע במשרד המשפטים, כולל טיפול בדרישות החוק.

כב. אחזקת הרשימות המעודכנות של הגורמים המחזיקים בנהלי אבטחת מידע.

כג. קיום מפגשים תקופתיים עם נאמני אבטחת מידע והנחייתם בהתאם לצורך.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, מטיל על גוף ציבורי את החובה למנות ממונה ביטחון, המופקד על "פעולות אבטחה פיזית", לרבות שמירה על רכוש, "פעולות לאבטחת מערכות ממוחשבות חיוניות" ו"פעולות לאבטחת מידע" לשם שמירה על מידע מסווג ומניעת פגיעה בו. כאמור, החוק אינו חל על הרשות המקומית, אך הוא מלמדנו על חשיבות הנושא ולדעת הביקורת רוח הדברים ודאי שחלה עליו.[32]

מבדיקה עם הרשות להגנת הפרטיות ניתן למנות ממונה על אבטחת מידע במיקור חוץ, אך עליו לעמוד בדרישות התקנות (כפיפות, אי ניגודי עניינים, יכולת וכו').

במסגרת "ניתוח העיסוקים", משרד הפנים פרסם תיאור לתפקיד "מנהל אבטחת מידע". לפי הגדרתו, להלן תחומי האחריות:

א. תכנון מדיניות אבטחת המידע ובקרה על יישומה.

ב. תכנון וביצוע סקרי אבטחת מידע.

ג. ניהול הרשאות, ודרכי הגישה למשתמשים.

ד. תכנון ויישום תוכנית התאוששות – DRP.

ה. ניהול ההגנה על מערכות המידע והתקשורת.

32 יש להזכיר שחוזר מיוחד של מנכ"ל משרד הפנים מספטמבר 2001 עוסק ב"ממונה על שירותי חירום ובטחון ברשויות מקומיות" והגם שתחום אבטחת המידע לא מתחומיו הנזכרים, מבקר המדינה בדוח לשנת 2011 על הרשויות המקומיות העיר שעל משרד הפנים לבחון אם יש מקום להנהיג את ההסדר האמור שנקבע לגבי גופים ציבוריים בחוק להסדרת הביטחון, שלפיו קציני הביטחון מופקדים על פעולות לאבטחת מידע ומערכות מידע, גם ברשויות המקומיות.

יצוין כי על פי הגדרת משרד הפנים – מנהל אבטחת המידע כפוף למנמ"ר (מנהל מערכות מידע ראשי) (שלא בהתאם ללשון החוק). מבקר המדינה העיר למשרד הפנים שנדרש לתקן את הכפיפות.

ממצאים

המועצה מינתה את הבעלים של החברה שמתחזקת את מחשוב המועצה כממונה אבטחה מידע. מינוי זה אינו על פי התקנות, שהרי כך שני התפקידים ותחומי אחריות מרוכזים אצל גורם יחיד באופן אשר מעמידו בניגוד עניינים. על הממונה לפקח על החברה המתחזקת (ומנהל מערכות המידע). מינוי זה הינו בניגוד לתקנה 3(4) לתקנות אבטחת המידע שלפיה: "הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה", אלא שהוסבר שמדובר באישיות נפרדת מהחברה ובמצב זמני.

זאת ועוד, לא הוכנה תוכנית סדורה לבקרה שוטפת.

המלצות

על המועצה למנות ממונה ואחראי אבטחת מידע, שתפקידיו יוגדרו מראש בהתאם לדין ובהתאם לצורך.

מומלץ שממונה ואחראי על אבטחת המידע יהיה כפוף למנכ"ל המועצה או לנושא משרה בכיר אחר, לא ימלא תפקיד נוסף ולא יעמוד במצב של ניגוד עניינים.

מומלץ לבחון ולהחליט בעניין חלוקת העבודה ושיתוף הפעולה בתחום זה עם קב"ט המועצה.

22. מינוי ממונה הגנה על הפרטיות

הרשות להגנת הפרטיות פרסמה המלצות בנוגע למינויים של ממוני הגנה על הפרטיות בארגונים וביחס לדרישות התפקיד.

לדעת הרשות להגנת הפרטיות, על מנת לשפר את מידת ההגנה על הפרטיות ולוודא עמידה בהוראות דיני ההגנה על מידע אישי, מומלץ למנות ממונה הגנה על הפרטיות שיופקד על יישום דיני ההגנה על מידע אישי בארגון.

"תפקידו המרכזי של הממונה הוא להביא להפנמה של עקרונות ושיקולי פרטיות בתהליכי העבודה בארגון ולסייע לארגון במימוש אחריותו וחובותיו לפי דיני הגנת הפרטיות.

מינויו של ממונה הגנת פרטיות באופן וולונטארי מהווה פרקטיקה ראויה ומומלצת (Best Practice) לארגונים האוספים ומעבדים מידע אישי.

פרקטיקה זו נושאת בחובה יתרונות רבים גם לארגונים וגם לציבור. הדבר עולה בקנה אחד עם האינטרסים הכלכליים של ארגונים במשק, שכן היכולת להגן על המידע האישי של הלקוחות או אנשים עליהם מחזיק הארגון במידע, הינה בעלת חשיבות כלכלית מובהקת. מינוי ממונה הגנת פרטיות יאפשר גם לציבור הלקוחות לרכוש אמון באשר לטיפול הארגון במידע האישי שלהם, ביודעם כי הארגון נקט ונוקט צעדים ממשיים לצמצום הסיכון לפגיעה בפרטיותם.

יתרון נוסף נוגע לארגונים רבים המכוונים לקהל לקוחות במדינות שונות בעולם. בידו של ממונה ההגנה על הפרטיות לסייע להנהלת הארגון להבין באילו מקרים ובאיזה אופן חוקים שונים שנחקקו ברחבי העולם הנוגעים להגנה על מידע, עשויים להשפיע על מהלך העסקים של הארגון, ולהיערך בהתאם.

במסמך ההמלצות מתייחסת הרשות להגנת הפרטיות להיקף תפקידו של הממונה אשר ייקבע על פי מורכבות פעולות עיבוד הנתונים המתבצעות בארגון ובהתאם לגודלו. כמו כן, התפקידים והמשימות שמומלץ שיהיו תחת טיפולו של ממונה הגנה על הפרטיות הם, בין היתר, הסדרת תהליכי ניהול מידע, פיקוח ובקרה והדרכה והטמעה.

על מנת שממונה ההגנה על הפרטיות יוכל לממש את אחריותו באופן מיטבי, מציינת הרשות כי יש לתת את הדעת לנושא סמכויותיו ועצמאותו של הממונה. כמו כן, נדרשים לו ידע והכשרה רלוונטיים. מומחיותו של ממונה ההגנה על הפרטיות נדרשת להיות משולבת, כך שתאפשר לו הבנה מיטבית של התהליכים בארגון ברמה הטכנולוגית והעסקית לצד יכולת לבחון את התאמתם לדרישות החוק ולמדיניות הארגון.

בנוגע למעמדו של ממונה הגנת הפרטיות בארגון ויחסיו עם בעלי תפקידים אחרים העוסקים בהגנה על מידע אישי - מציינת הרשות כי מומלץ שהממונה יהיה חלק מההנהלה הבכירה של הארגון, כמינוי פנימי של עובד החברה או גורם חוץ. ככל שמדובר במינוי פנימי, ראוי שהעובד לא יהיה נתון לניגוד עניינים עקב תפקיד אחר שהוא ממלא בארגון. ככל שמדובר בארגון גדול, או כאשר ליבת העיסוק של הארגון כרוכה בעיבוד מידע אישי, או במקרים בהם מעובד מידע אישי בקנה מידה רחב, רצוי כי ממונה הגנת הפרטיות יהיה מינוי פנימי ובעל תפקיד בכיר בארגון. ככל שמדובר בארגון בינוני או קטן, שליבת עיסוקו אינה כרוכה בעיבוד מידע אישי, קיימת אפשרות למנות ממונה חיצוני, שאינו עובד הארגון".[33]

ראוי להביא מדברי הסיכום של הרשות להגנת הפרטיות במסמך הסבר בנושא זה:

"החוק הישראלי אינו מטיל כיום חובה כללית למינוי ממונה ארגוני להגנה על הפרטיות. אולם, עמדת הרשות היא כי הסמכה של ממונה הגנה על הפרטיות היא אמצעי ראשון במעלה לשיפור רמת הציות לדיני הגנת המידע בארגון, לקידום האחריותיות ביחס לניהול מידע אישי בו, לקיום דרישת המידתיות בפעילות בעלת פוטנציאל לפגיעה בפרטיות,

[33] https://www.gov.il/he/Departments/publications/reports/dpo_doc_kit

ולשמירה מיטבית על הזכות לפרטיות בארגון. יתרה מזו, מינוי ממונה הגנת פרטיות ארגוני עולה בקנה אחד גם עם האינטרס הפנימי של הארגון .שכן, יכולת הארגון להגן על המידע האישי של נושאי המידע היא בעלת חשיבות כלכלית של ממש. מינוי ממונה הגנת פרטיות מאפשר לנושאי המידע לרכוש אמון באשר לטיפול במידע האישי שלהם, ביודעם כי הארגון נקט ונוקט צעדים לצמצום הסיכון לפגיעה בפרטיותם. כמו כן, תפקידו של הממונה כולל בין היתר הקמת ערוץ תקשורת מול הרשות להגנת הפרטיות. ממונה הבקיא בתהליכי העבודה מול הרשות יאפשר לארגון המתמודד עם הפרה לנהל את האירוע באופן יעיל מול הגורמים המקצועיים, ובמקרים המתאימים גם מול הרשות עצמה, ובכך לחסוך עלויות גבוהות. יתרון נוסף נוגע לארגונים רבים המכוונים לקהל לקוחות במדינות שונות בעולם. ממונה ההגנה על הפרטיות יכול לסייע להנהלת הארגון להבין באילו מקרים וכיצד חוקים שונים שנחקקו ברחבי העולם הנוגעים להגנה על מידע, עשויים להשפיע על מהלך העסקים של הארגון, ולהיערך בהתאם. לאור האמור לעיל, קיימת חשיבות גדולה למינוי של ממונה הגנה על הפרטיות בארגון לצורך יישום אפקטיבי של דיני ההגנה על מידע אישי בישראל. מעבר לכך, מינוי אדם בעל הבנה מעמיקה בדיני ההגנה על מידע אישי, ובאופן היישום של דינים אלו, יחסוך לארגון זמן וכסף וימנע טעויות יקרות".[34]

ממצאים

במועצה לא שמעו על תפקיד ממונה הגנה על הפרטיות. לשאלת הביקורת, מאחר ואין חובה חוקית לכך ואין תקציב עודף, לא מתכוונים למנות בקרוב תפקיד כזה.

המלצות

אכן אין חובה ישירה בחוק[35] למינוי ממונה הגנת הפרטיות ומדובר במינוי וולונטרי, ועדיין לדעת הביקורת, מומלץ למועצה לפעול למינוי כאמור.

זאת לאור החובות בתחום אבטחת המידע והגנת הפרטיות ולאור הסיכונים השונים – משפטיים, תפקודיים ואחרים – העולים מאי הקפדה על הנדרש.

מובן שאין להתעלם מההיבט התקציבי, אך בתור התחלה ניתן למנות עובד קיים ולפעול כך שמינוי זה לא יעמיס מבחינה תקציבית על המועצה. זאת ועוד, תפקיד כזה, עשוי לצמצם סיכונים וגם לחסוך תקציבית.

34 https://www.gov.il/BlobFolder/reports/dpo_doc_kit/he/dpo_doc.pdf

35 בחוות הדעת של הרשות להגנת הפרטיות נאמר, כי "לאור תחולתה האקס-טריטוריאלית של הרגולציה האירופית, ובשל העובדה כי ה GDPR-משמשת מקור השראה לחקיקת פרטיות במדינות רבות, מינוי ממונה הגנת פרטיות עשוי להיות ממילא חובה חוקית ישירה בארגון ישראלי הכפוף לרגולציה זרה..".

<u>תיקון ליקויים מדוח 2015</u>

הביקורת ביצעה ביקורת בתחום אבטחת מידע כבר בשנת 2015 בתחומים הבאים:

1. נהלים
2. ממונה ואחראי אבטחת מידע
3. ועדת היגוי לתחום אבטחת המידע
4. תקצוב אבטחת מידע
5. הדרכה וקיום אבטחת מידע אצל עובדים
6. הדרכה וקיום אבטחת מידע אצל נותני שירות ומיקור חוץ (outsourcing)
7. תחום הגיבוי – הגופים החיצוניים והמועצה
8. חומת אש (FireWall), ואנטי וירוס
9. רישוי תוכנות
10. אתר האינטרנט של המועצה
11. אבטחה פיזית
12. מערכות אל-פסק
13. בטיחות אש ומים
14. אבטחה לוגית
15. ניטור יומן השימוש - (log)
16. סיסמאות
17. אבטחת מידע במחשבים מנותקי רשת ובהתקני אחסון ניידים
18. מצלמות מעקב
19. תוכנית שיקום מאסון ותוכנית המשכיות עסקית
20. הטיפול ברשומות "מידע מוגבל" ו"מידע רגיש"
21. מחלקת החינוך ויחידת השירות הפסיכולוגי החינוכי
22. מחלקת רווחה ושירותים חברתיים
23. אבטחת מסמכים במחלקת הגבייה
24. טיפול במידע היוצא מהמועצה
25. סדרי העברת מידע בין גופים ציבוריים והחזקת מידע
26. רישום מאגרי מידע ברשם מאגרי המידע

במספר תחומים חלו שיפורים (בעיקר בתחום הגיבוי, חומת האש ואנטי וירוס, רישוי תוכנות, מצלמות מעקב, רישום מאגרי מידע). מחמת הזמן הרב שעבר, פרסום תקנות אבטחת המידע החדשות, עדכוני נהלים והנחיות, חלק מהדברים אינו רלבנטי ולכן אין צורך בבדיקת תיקון כל הליקויים. יש לציין, כי חלק ניכר עדיין רלבנטי וליקויים לא תוקנו באופן מלא בכל התחומים כמפורט לעיל וכפי שבאו לידי ביטוי לאורך דוח זה.

מרחב הסייבר נתון בסכנה מתמדת עם מגמה בינלאומית לעלייה בסכנות, באיומים ובנזקים.

פגיעה במרחב הסייבר עלולה להסב נזקים כבדים לצנעת הפרט, למסחר, לתקינות וליעילות התפקודית, הארגונית והניהולית.

הסיכונים המהותיים הם בתחום אבטחת המידע ופרטיות התושבים.

המועצה האזורית לכיש עושה שימוש הולך וגובר בטכנולוגיה, באתר האינטרנט שלה ובאינטראקציה מקוונת כגון תשלומים, העברת מידע וקבלת מידע.

התלות של המועצה במערכות הממוחשבות ובמאגרי המידע הולכת וגדלה ועימה הצורך בהגנה על מרחב הסייבר.

מאגרי המידע של המועצה מכילים פרטים אישיים וסודיים רבים, ולכן פגיעה בהם ובמידע האצור בהן או חשיפתם, עלולה לפגוע בפרטיות ולהסב נזקים שונים.

לאור דברים אלו, על המועצה לנקוט צעדי אבטחת מידע שונים לצמצום הפגיעה במרחב הסייבר וכמובן להקפיד על עמידה בהוראות הדין.

מבדיקת הביקורת עולה, כי ככלל, המועצה אינה עומדת בכללי אבטחת המידע החלים עליה, והיא חשופה לסיכונים שונים משפטיים, כלכליים ותפעוליים.

ניתן לקבוע, כי למועצה אין אסטרטגיה כוללת לניהול מערכות המידע, אין תוכניות עבודה מסודרות ולא מתבצעת פעולה סדירה ורציפה בנושא.

כבר כאן יצוין לטובה ממונה אבטחת המידע אשר עושה כמירב יכולתו במשאבים המצומצמים - של זמן, משאבי אנוש ותקציב - העומדים לרשותו והוא מתריע על חשיבות הנושא.

הממצאים מעלים ליקויים באשר לעמידה בהוראות הדין בתחום אבטחת המידע, ניהול מאגרי המידע ושמירת הפרטיות.

כך למשל התברר כי המועצה לא עומדת בכללים בעניין מאגרי המידע כמו מיפוי, רישום וניהול סיכונים; לא קיימים נהלי עבודה בנושא אבטחת מידע; לא הוכנה תוכנית לבקרה שוטפת על העמידה בדרישות התקנות; למועצה אין תוכנית סדורה ומאושרת להתמודדות עם אירועי סייבר; לא מבוצע ניטור רציף כולל ומסודר; אין הקפדה מלאה על אבטחת מידע ופרטיות על מיקור החוץ; מינוי ממונה אבטחת המידע אינו לפי התקנות ובחשש לניגוד עניינים תפקידי.

הביקורת מברכת על פעילות המועצה בתחומי התשתית, אולם לצורך אבטחת מידע נאותה והגנת הפרטיות באופן ראוי, יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים ייעודי.

יצוין לטובה ממונה אבטחת המידע אשר פועל לעליית מדרגה בתחום המחשוב באופן כללי, בעיקר בתחום התשתית, שמהווה בסיס לשיפור נושא אבטחת המידע. כמו כן,

הממונה דואג למעקב אחר רישוי ועדכון תוכנות, חומת אש ואבטחת מידע באמצעים ובזמן המועט שלרשותו. זאת ועוד, הממונה מסר כי העביר מסר בדבר הצורך

ממצאי הביקורת מלמדים כי במועד סיום הביקורת הנוכחית, כשבע שנים לאחר שבוצעה הביקורת המשמעותית הקודמת, המועצה רחוקה מלעמוד ברמה גבוהה או מספקת של אבטחת מידע ושמירה על הפרטיות, וודאי שלא ברמה הנדרשת. הליקויים חושפים את המועצה לסיכונים שונים בתחום אבטחת המידע ובאופן כללי לפגיעה בפרטיות, ברציפות וביעילות התפקודית כמו גם חשיפה לתביעות.

על המועצה לתקן את הליקויים שהועלו בדוח זה בנוגע לפעולותיה בתחום אבטחת המידע והגנת הפרטיות, לפעול לפי מדיניות סדורה וכוללת, לפעול לרמה תשתיתית וטכנולוגית מתאימה, להעלות את המודעות לחשיבות הנושא בקרב העובדים ולהעמיד לרשותם את האמצעים הנדרשים.

<u>בין היתר ו"על קצה המזלג":</u>

על המועצה לעמוד בכללים בעניין מאגרי המידע כמו ביצוע מיפוי למאגרי המידע הקיימים אצלה, רישום המאגרים וניהול סיכונים; להכין ולהסדיר נוהל מפורט בהתאם לדין, ומומלץ שאף מעבר לו בנושא אבטחת המידע ולעדכנו מעת לעת לפי הצורך; לעבוד נכון בעניין מיקור חוץ; מלבד הצורך במינוי ממונה אבטחת מידע מתאים ובהיקף העסקה ראוי, הומלץ להקים ועדת היגוי בליווי גורם מקצועי לצורך אבטחת מידע ושמירת הפרטיות; המועצה התקדמה בעניין התשתיות, אך בנוסף לכך, יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים מספיק; על המועצה באמצעות ממונה אבטחת המידע להכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, להוציא אותה לפועל ולהודיע כאמור על הממצאים. כמו כן, מומלץ למועצה להכין תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית עם כל הפעולות הנלוות; ראוי כי המועצה תתקצב את אבטחת המידע בסעיף תקציב ייעודי כחלק יחסי מתקציב המחשוב ומערכות המידע. מומלץ לבחון את גובה תקצוב לאור ממצאי הביקורת ולקבוע אותו בהתאם לייעוץ שיינתן למועצה בנושא; מומלץ שהמועצה תנקוט פעולות להגברת המודעות, החשיבות, הסיכונים והאיומים בתחום אבטחת המידע. כך, על המועצה לקיים פעולות הדרכה והסברה בתחום אבטחת המידע ושמירת הפרטיות; מומלץ לבחון היטב את ההגנה הארגונית גם ברמה המחלקתית והגנת תחנות הקצה ולתקן את הדרוש תיקון כולל מידור נדרש בין תחנות; על המועצה להיערך באופן מסודר תוך הכנת תוכנית ראויה למצב של התאוששות מאסון. תוכנית כזו תסייע למועצה להמשיך לתפקד כראוי ולהתמודד טוב יותר עם אירועי סייבר כגון גניבת מידע, פריצה למאגרים, מחיקת מידע ועוד; על המועצה לפעול בהתאם לתקנות ובהתאם לצורך באשר לניהול ההרשאות, לגישה, לזיהוי ולאימות ולניטור; בכל הקשור ל"עיר (מועצה) חכמה" ולהטמעת טכנולוגיות חדשות, מומלץ למועצה לגבש מסקנות והחלטות רק לאחר היוועצות בגורמי מקצוע, לימוד הצורך והכרת ההזדמנויות והסיכונים; על

המועצה למנות ממונה ואחראי אבטחת מידע, שתפקידיו יוגדרו מראש בהתאם לדין ובהתאם לצורך. מומלץ למועצה לפעול למינוי ממונה הגנת הפרטיות, למרות שאין לכך חובה ישירה בחוק.

הנה כי כן, על המועצה להגביר את עמידותה הן בפני פגיעה במערכות המידע שלה ובפרטיות והן לצורכי הגנה על רציפות תפקודית ותפעול כלל השירותים לטובת הציבור.

על מנת לפעול כראוי בתחום אבטחת המידע והפרטיות, על המועצה לפעול בהתאם לדיני אבטחת המידע והגנת הפרטיות והביקורת המליצה על הפעולות הנדרשות גם מעבר למחויב על פי דין.

1. מסמך הגדרות מאגר

ממצאים

המועצה לא מיפתה את מאגרי המידע הרלוונטיים לחוק הגנת הפרטיות ולא הוכנו מסמכי "הגדרת מאגר" כנדרש בתקנות.

המלצות

עריכת מסמך הגדרת המאגר, תסייע למועצה להגדיר מהי רמת האבטחה החלה עליה, שלה תלות במספר בעלי ההרשאה למאגרי המידע במועצה, במספר האנשים עליהם שמור מידע במאגרים ובאופי המידע השמור.

על המועצה, המנהלת מאגרי מידע על תושביה, הכוללים אפיון נושאי המידע לרבות מידע עליהם, לבצע מיפוי לכל מאגרי המידע הקיימים אצלה, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים ולעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

2. רישום מאגרי מידע

ממצאים

משיחות עם עובדי מועצה וממונה אבטחת המידע נמסר, כי אין מאגרים רשומים או כי לא ידוע על כאלה. הרשות להגנת הפרטיות מסרה, כי קיימים חמישה מאגרים רשומים. מסתבר שהרישום לוקה בחסר, אינו מעודכן ומכיל פרטים לא נכונים. להלן שמות המאגרים וחלק מהפרטים:

א. תיקים אישיים בהנהלת חשבונות. לא רשום שם מנהל מאגר. נרשם בשנת 2011.

ב. גביה. נרשם בשנת 2011. כמנהל המאגר רשום שם של גזבר המועצה שהפסיק את תפקידו בשנת 2005 (לפני כ-17 שנים). לא ברור כיצד המאגר נרשם על שמו.

ג. שכר ומשאבי אנוש. נרשם בשנת 2013. כמחזיקה רשומה החברה לאוטומציה.

ד. שכר וכח אדם. נרשם בשנת 2011. כמנהלת המאגר רשומה עובדת מועצה שפרשה בשנת 2017.

ה. מערכת פיננסית. נרשם בשנת 2013. לא רשום מנהל מאגר. כמחזיקה רשומה החברה לאוטומציה.

מלבד המאגרים הנ"ל שרישומם לא מעודכן, המועצה טרם רשמה את מאגרי המידע אצל רשם המאגרים כנדרש בסעיף 8 בחוק.

יצוין, כי משיחת הביקורת עם נציגי הוועדים המקומיים, עולה כי אין מודעות לחובות הוועדים בתחום מאגרי המידע ובכלל בתחום אבטחת המידע. ניתן לומר כבר כאן, כי בכל נושא שבו מתואר כשל של המועצה בתחום אבטחת המידע, הדברים נכונים גם לגבי הוועדים המקומיים בתחום חובותיהם לפי דין.

המלצות

רישום המאגרים נועד להבטיח את הגנת הפרטיות של מאגרי המידע ולתת כלים, הן לרשם מאגרי המידע והן לציבור שהמידע עליו מנוהל במאגרי המידע, וכך ניתן לאכוף את הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי המאגרים.

במצב בו אין נהלים ואין יישום של הדין בנושא, מומלץ, כי המועצה תבחן מה עליה ליישם מדיני הגנת הפרטיות, תמפה את מאגריה ותפעל בהתאם לכל הוראות הדין.

כך וכאמור, על בסיס המיפוי הנדרש כאמור לעיל, על המועצה לרשום מאגרי מידע שאינם רשומים, לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע וכו'.

ההמלצה האמורה נכונה גם לגבי הוועדים המקומיים שעליהם לוודא את קיום הוראות הדין בתחום מאגרי המידע ובכלל בתחום אבטחת המידע. הדברים לגבי הוועדים מוזכרים כאן, אך נכונים לאורכו של הדוח.

3. חובת מבקש מידע, זכות העיון ותיקון מידע

<u>ממצאים</u>

ככלל, בתחומים שונים כמו חינוך, רווחה וגביה, המועצה אינה מקפידה על שקיפות בנוגע למקור הסמכות לאיסוף המידע האישי על התושבים, ואינה מקפידה על יידוע התושבים שעליהם מוחזק המידע בדבר זכויותיהם בנוגע למאגר המידע בו נשמרים פרטיהם, בהתאם לסעיף 11 לחוק בעת פניה לקבלת מידע מהתושב. לא נמצא יידוע לתושבים ולנושאי המידע בדבר האפשרות לעיין במידע כנדרש בסעיף 13 לחוק ולא בדבר האפשרות לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק.

המלצות

על המועצה ליידע את התושבים בדבר המקור החוקי לאיסוף המידע אודותיהם, וכאשר אין סמכות חוקית כזו, לקבל את הסכמת התושב עבור שמירת פרטיו במאגריה. זאת, עם מתן הודעה לתושבים בעת איסוף המידע, הכוללת התייחסות

לשאלה האם חלה עליהם חובה חוקית למסור את המידע כאמור, או שהיא נתונה לרצונם והסכמתם, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע והמטרה. כמו כן, על המועצה להקפיד לאפשר לתושבים לעיין במידע אודותיהם, בהתאם להוראת סעיף 13 לחוק. זכות עיון זו חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות למוקד, פניות לאתר, שיחות זום ואחרות מצולמות בווידאו וכיו"ב או שמירת צילומים אחרים, אשר נשמרים באופן דיגיטלי על ידי המועצה או גוף אחר הנותן שירות לציבור. כמו כן, יש להקפיד ולאפשר לתושבים לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע בהתאם לסעיף 14 לחוק, כאשר המידע אינו נכון, שלם, ברור או מעודכן.

4. נהלי אבטחת מידע

ממצאים

במועצה לא קיימים נהלי עבודה בנושא אבטחת מידע כנדרש בתקנות.
יצוין, כי כבר בשנת 2015, לפני כניסתן לתוקף של תקנות אבטחת המידע, הביקורת המליצה לקבוע נוהל שיכלול בעיקר את המרכיבים הבאים:

- מבנה מאגר המידע ורשימת מצאי;
- תיאור אמצעי ההגנה על מערכות המחשוב ותשתיות התקשורת;
- סמכות ואחריות;
- הדרכה והוראות למורשי גישה למערכת, לגבי אופן השימוש במערכת תוך אבטחת המידע;
- תיאור רכיבי המערכות ותיאור מבנה הרשת;
- הסיכונים להם חשוף המידע;
- תיאור אופן מתן הרשאות גישה למערכת ואופן ביטולן;
- הוראות בדבר אופן אימות זהותם של מורשי גישה למערכת ואופן הטיפול בתקלות באימות זהות;
- הוראות לעניין רמת אבטחת הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות;
- הוראות בדבר אבטחה פיזית וסביבתית;
- ניתור ובקרה על שימוש במערכות המידע; הוראות בדבר עבודה עם גורמי חוץ;
- הוראות בדבר ניהול והעברה של אמצעי אחסון והתקנים ניידים;
- הוראות בדבר אופן גיבוי מידע, שחזורו ואופן התמודדות עם אירוע אבטחה;
- הוראות בדבר ביצוע ביקורות תקופתיות וסקר סיכונים לשם הבטחת קיומם ותקינותם של אמצעי האבטחה; אופן התמודדות עם אירועי אבטחה;
- הוראות בדבר חובת דיווח למנהל על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

- תוכן הנוהל שהוצע, התבסס, בין השאר, על גרסת טיוטה של תקנות אבטחת מידע לפני שנכנסו לתוקף. הומלץ למועצה ללמוד מטיוטת התקנות, אך הדבר לא נעשה.

המלצות

על המועצה להכין ולהסדיר נוהל מפורט בהתאם לדין, ומומלץ שאף מעבר לו בנושא אבטחת המידע ולעדכנו מעת לעת לפי הצורך.

עובר לקביעת הנהלים, מומלץ להיוועץ בגורמי מקצוע ולקבוע מדיניות אבטחה.

5. מסירת מידע או ידיעות מאת גופים ציבוריים

ממצאים

במועצה לא מיושמים הכללים בדבר מסירת מידע או ידיעות מאת גופים ציבוריים.

המלצות

מומלץ, כי המועצה תקבע מדיניות והגדרות לגבי העברת המידע לגופים ציבוריים.

על המועצה ליישם באופן מיידי את הוראות החוק והתקנות בעניין מסירת מידע או ידיעות מאת גופים ציבוריים. מומלץ למועצה לוודא קיום הוראות הדין גם באשר למידע שמקבל אצלה מגופים אחרים.

6. ועדת היגוי לתחום אבטחת המידע

ממצאים

במועצה אין צוות היגוי או צוות חשיבה כלשהו אשר עוסק באופן ממוקד בנושא אבטחת מידע.

ממונה אבטחת המידע פועל לעליית מדרגה בתחום המחשוב באופן כללי, בעיקר בתחום התשתית, שמהווה בסיס לשיפור נושא אבטחת המידע.

בתוך כלל הפעולות הוזכר נושא אבטחת המידע והממונה עמד על חשיבותו, אך הנושא לא תוקצב ולא טופל באופן ייעודי.

שיפור התשתיות במועצה מהווה תנאי הכרחי, אך לא מספיק לאבטחת המידע.

הביקורת מברכת על פעילות המועצה בתחומי התשתית, אולם לצורך אבטחת מידע נאותה יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים ייעודי.

מבדיקת פעולות המועצה בתחום התשתיות עולה, כי התשתיות המשופרות עשויות לסייע למועצה באפשרות לעלות מספר קומות בתחום אבטחת המידע. בין היתר, התשתיות המשופרות עשויות להגביר את רמת הקונקטיביות בין האגפים, להגביר ולאחד את רמת האבטחה, לשפר את תעבורת הנתונים ולבקרה, להוסיף שרתים ואמצעי אבטחה, לנהל את התחנות האישיות ולשלוט עליהן ברמה הנדרשת, וכן להתקין אמצעי ניטור ובקרה.

כל אלו לא ייעשו מעצמם. התשתיות המשופרות מהוות תנאי, אך אין בכך די. הביקורת לא מצאה מדיניות ותוכניות ארוכות טווח העוסקות בכל אלו. הביקורת לא מצאה גוף ניהולי העוסק בתחום ברמה הכוללת, מלבד ממונה אבטחת מידע, המועסק באופן מצומצם ביותר ושלא מספיק לראייה כוללת והתוויית מדיניות, שהוא בעלים של החברה שנותנת שירות (על כך להלן).

המלצות

אכן, תשתיות המחשוב והתקשורת המשופרות במועצה, מהוות קפיצת מדרגה גם בתחום אבטחת המידע, אך אין בכך די. לדעת הביקורת, על המועצה להמשיך ביתר שאת בפעולותיה גם בהתמקדות באבטחת המידע ושמירת הפרטיות.

כשם שבתחום הבטיחות בתחבורה אין די בתשתיות ראויות ויש צורך בראייה כוללת ופעולות בתחומים מגוונים על מנת להתמודד, לייעל ולשפר את הבטיחות, כך בתחום אבטחת המידע, בנוסף לפעילות בתחום התשתיות, יש צורך במבט מכלולי, ניהולי ומקצועי ובארגז כלים מספיק.

מלבד הצורך במינוי ממונה אבטחת מידע מתאים ובהיקף העסקה ראוי, על אף שהחוק לא מחייב, הביקורת ממליצה להקים ועדת היגוי בליווי גורם מקצועי לצורך אבטחת מידע ושמירת הפרטיות, שתדון במכלול תחומי אבטחת המידע ברמה הניהולית הכוללת ובין השאר, בנושאים העולים בדוח זה.

מומלץ שוועדת ההיגוי תתווה מדיניות, תפעל להקצאת משאבים נאותה, תסקור את הקיים, לפעל לשיפור וייזום, תאשר תוכניות עבודה, תקבל דיווחים ותעקוב באופן שוטף אחר ביצוע.

7. תוכנית לבקרה שוטפת ובכלל בתחום המחשוב

ממצאים

במועצה לא הוכנה תוכנית לבקרה שוטפת על העמידה בדרישות התקנות. מנהל מערכות המידע מסר, כי בתכנון להכין תוכנית מקפת הן בתחום הרכש וההצטיידות והן בתחום אבטחת המידע. הדברים ייצאו לפועל לאחר אישור המועצה.

הגם שחלק זה לא מיועד לשעת חירום, יוער, כי לא הוכנה בידי בעלי מקצוע בתחום המחשוב תוכנית לשעת חירום בתחום אירועי הסייבר.

המלצות

על המועצה באמצעות ממונה אבטחת המידע להכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, להוציא אותה לפועל ולהודיע כאמור על הממצאים.

כמו כן, מומלץ למועצה לפעול בהתאם להנחיות תורת ההגנה ובכלל זה קביעת תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית עם כל הפעולות הנלוות כאמור.

מעבר לתוכניות השונות העולות בדוח זה שעל המועצה להכין, על המועצה להכין תוכנית לשעת חירום בתחום אירועי הסייבר.

8. מיפוי מערכות המאגר, ביצוע סקר סיכונים וביקורות תקופתיות

ממצאים

במועצה אין מדיניות סדורה באשר למיפוי, סקר סיכונים ובקרה. במועצה לא בוצע מיפוי של מערכות המאגר כנדרש, לא בוצעו סקר סיכונים מקיף ומפורט בתחום אבטחת המידע, כמעט ולא בוצעו מבדקי חדירה ולא מבוצעות בקרות תקופתיות. יוער, כי באמצעות ממונה אבטחת המידע שהינו גורם מקצועי ומבין המצב יותר טוב מזה שהיה בבדיקת הביקורת בשנת 2015, אך התקציב העומד לרשותו לא מאפשר לו להמשיך לרמה הנדרשת.

המלצות

על מנת שהמועצה תעמוד בתקנות אבטחת המידע ותהיה מוכנה לטיפול בחולשות ובסיכונים במערכות המחשוב והמידע, עליה לבצע סקרי סיכונים, מבדקי חדירה וביקורות תקופתיות.

הביקורת ממליצה למועצה לקבוע עקרונות ומתודולוגיה לניהול סיכונים בתחום אבטחת המידע, לנהל באופן שוטף את הסיכונים, לבצע מבדקי חדירה בהתאם לדין ולצורך (לפי רמת המאגר), לקבוע נהלים בתחום, לקבוע סמכויות ותחומי אחריות ולבצע בקרות.

ייתכן וראוי לפעול לגבי כלל המאגרים כמו שיש לפעול בעניין המאגרים שחלה עליהם רמת אבטחה גבוהה, שכן בכל המאגרים תיתכן פגיעה בפעילות השוטפת של המועצה וברמת השירות, וזאת מעבר לפגיעה בפרטיות.

9. תקצוב אבטחת מידע

ממצאים

הביקורת העלתה, כי במועצה לא הוצגו להנהלה ולא נקבעו תקציבים ייעודיים לאבטחת מידע, אלא הם נכללים בסך תקצוב המחשוב.

המלצות

לדעת הביקורת, ראוי כי המועצה תתקצב את אבטחת המידע בסעיף תקציב ייעודי כחלק יחסי מתקציב המחשוב ומערכות המידע. מומלץ לבחון את גובה תקצוב לאור ממצאי הביקורת ולקבוע אותו בהתאם לייעוץ שיינתן למועצה בנושא.

10. הדרכה וקיום אבטחת מידע אצל עובדים

ממצאים

המועצה לא נוקטת אמצעים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר. עובדים חדשים או כל גורם שמקבל גישה למאגר או למערכות המאגרים, אינם עוברים תהליך מיון ולא נבדקת התאמתם לקבלת הגישה למאגרי המידע.

אגף הסייבר במשרד הפנים קיים הדרכות בנושא אבטחת מידע באמצעים מקוונים לעובדי רשויות, אך המועצה לא תיאמה הדרכה כזו.

המועצה לא מקיימת פעולות הדרכה והסברה בתחום אבטחת המידע לעובדים. מבדיקת הביקורת עולה, כי לא התבצעו פעולות הדרכה המתאימות לעת סיום יחסי עבודה של עובדים.

המלצות

על המועצה לתת גישה למידע המצוי במאגריה או לשנות היקף הרשאה שניתנה, רק לאחר שתנקוט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה מתאים לקבלת גישה למידע המצוי במאגר.

על המועצה לקיים פעולות הדרכה והסברה בתחום אבטחת המידע בדומה לדרישות המפורטות בנוהל המסגרת או לפי נוהל מתאים שתקבע לנכון,[36] וזאת עד שתצאנה הנחיות מסודרות ממשרד הפנים, משרד המשפטים או מגורמי רגולציה אחרים.

על המועצה לגבש תוכנית הדרכה כוללת להגברת מודעות העובדים בכל ההיבטים הנוגעים לאבטחת מידע ובכלל זה הדרכה בנהלי המועצה בתחום זה וריענון מעת לעת כולל תיעוד לגבי כל עובד.

מומלץ שהמועצה תנקוט פעולות להגברת המודעות, החשיבות, הסיכונים והאיומים בתחום אבטחת המידע.

36 מלבד הדרכה כללית, ממונה אבטחת המידע הציע הדרכה לבכירים, מנהלים ועובדים.

11. חומת אש (FireWall), אנטי וירוס ואבטחת תקשורת

ממצאים

מדיניות הגלישה מתירנית ביותר. אין חסימה לקטגוריות מסוכנות.

משתמשי הקצה יכולים להתקין להתקין תוכנות ולבצע מגוון שינויים בהגדרות כמעט ללא פיקוח.

נושא חומת האש ואנטי וירוס נבדק בשנת 2015. אבטחת המידע הלוגית מתקיימת, בין היתר, באמצעות "חומת אש" (FireWall), ואנטי וירוס של eset.

בזמנו, במהלך הביקורת התברר כי לא כל תוכנות האנטי וירוס מעודכנות. המצב תוקן באופן מיידי. ממונה אבטחת המידע מסר, כי כיום המצב תקין והוא דואג לעדכונים כנדרש.

הביקורת לא הצליחה לוודא הגנה ראויה לתחנות הקצה.

אין התייחסות מיוחדת להעברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט ולגבי גישה מרחוק (מנהל מערכות המידע יכול לגשת בקלות לכל מחשב ללא כל יידוע משתמש הקצה).

מנהל מערכות המידע, מסר כי הוא דואג לעדכן את מערכות התוכנה. בתחום החומרה היה רוצה לעדכן יותר, אך מדובר בנושא תלוי תקציב.

אין הגנה מיוחדת על הטלפונים הניידים במועצה.

המלצות

יש להמשיך לעדכן ולעקוב באופן שוטף אחר רמת חומת האש (FireWall) והאנטי וירוס במועצה ובכלל זה דאגה מתמדת להתקנת עדכונים מיד עם פרסומם.

מוצע להיוועץ בגורם חיצוני באשר למדיניות הגלישה, מרחב השימוש של משתמש הקצה, לגבי העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, לגבי מאגרים שניתן לגשת אליהם מרחוק, שימוש בשיטות הצפנה מקובלות, בחינת מוצרי האבטחה הקיימים ובכלל זה בחינת צורך בשדרוג והוספת כלי אבטחה וכו'.

על מנת לנטרל מראש חולשות ופגיעות, על המועצה לעדכן באופן שוטף את מערכות המאגרים, התוכנה והחומרה בהתאם להנחיות היצרן ולצורך.

מומלץ לבחון היטב את ההגנה הארגונית גם ברמה המחלקתית ושל תחנות הקצה ולתקן את הדרוש תיקון כולל מידור נדרש בין תחנות.

מומלץ לבצע הגנת אבטחת מידע לטלפונים הניידים במועצה.

מומלץ להיוועץ עם גורם מקצועי לצורך הגברת האבטחה באופן כללי ובהקשר דנן גם לאבטחת גישה מרחוק.

12. שמירה, גיבוי ושחזור של נתוני אבטחה

ממצאים

מנהל מערכות המידע מסר, כי הוא ערוך להתמודדות עם אירועי סייבר ככל שהתקציב מאפשר. למועצה אין תוכנית סדורה ומאושרת להתמודדות עם אירועי סייבר.

למועצה אין נוהל גיבויים כנדרש. מנהל מערכות המידע דואג לביצוע גיבויים, אך הוא לא מלא (כך למשל נמסר ממשתמשים במחשבים ניידים שלא ערכו גיבוי שוטף).

המלצות

ככלל, לאורך דוח זה עולה הצורך של המועצה להכין תוכנית עבודה כוללת ואסטרטגית שתשמש בסיס לתוכניות עבודה שנתיות. בכלל זה תוכנית להתאוששות מאסון.

על המועצה לפעול לפי מתווה משרד הפנים. מומלץ למועצה לפעול בהתאם לתורת ההגנה, ובכדי לגבש תוכנית עבודה לשיפור ההיערכות לעניין ההגנה מפני אירועי סייבר, להגדיר על מה המועצה נדרשת להגן, מהי רמת ההגנה הנדרשת, ובאילו תחומים עליה להשתפר כדי להגיע לרמה זו.

על המועצה להיערך באופן מסודר תוך הכנת תוכנית ראויה למצב של התאוששות מאסון. תוכנית כזו תסייע למועצה להמשיך לתפקד כראוי ולהתמודד טוב יותר עם אירועי סייבר כגון גניבת מידע, פריצה למאגרים, מחיקת מידע ועוד.

מומלץ למועצה לבחון היטב את הצורך ובהתאם לכך להיערך גם תקציבית.

13. רישוי תוכנות

ממצאים

בשונה מהמצב המתואר בדוח 2015 בו היו מספר עמדות ללא רשיונות או עם רשיונות לא מעודכנים ולא נערך מעקב (כבר אז המצב תוקן), מממונה אבטחת המידע נמסר, כי ממשיכים להקפיד על כך ומתבצע מעקב.

המלצות

הביקורת ממליצה, כי מעת רכישה והתקנה יוודא נושא הרישוי ויתועד באופן מסודר, ממוחשב וברור.

מובן, שמנהל אבטחת מידע וקיום נהלים וגורמי סיוע אחרים, אשר נידונים בדוח זה יסייעו וידאגו גם הם לתקינות בתחום הרישוי.

14. אבטחה פיזית וסביבתית

ממצאים

יצוין, כי הביקורת העלתה ליקויים בנושא זה בדוח 2015. אומנם המצב טוב יותר (פחות גישה פיסית), אך עדיין לא במצב שפיר לפי התקנות.

הביקורת בחנה את האבטחה הפיזית והסביבתית של מקום ארונות התקשורת והשרתים בהם נשמרים המאגרים (ישנם מאגרים אחרים שנשמרים בענן).

נמצא כי הסביבה הפיזית בה נשמרים ארון התקשורת והשרתים של המועצה אינם אינה הולמת ואינה עומדת בדרישות התקנות.

דוג' לליקויים ממוקדים: בחדר השרתים לא קים תיעוד הנכנסים ואת הנעשה בחדר; אין הרשאות כניסה לחדר; לא קיים חיישן טמפרטורה; היעדר מערכת כיבוי אש; היעדר התראות לאחראי ברשות בעת אירוע הדורש טיפול מיידי, כגון כניסת בלתי מורשים לחדר השרתים, שרפה, תקלות טכניות, תקלות חשמל, הפסקת תקשורת וכו'; אין התייחסות ביטחונית מיוחדת.

המלצות

על המועצה לקיים את הוראות התקנות בעניין האבטחה הפיזית והסביבתית.

בשלב ראשון ומיידי, רצוי להתקין קודן, מצלמות אבטחה ודלת מתאימה. בהמשך ראוי להיוועץ בגורם מקצועי ולפעול בהתאם.

15. ניהול הרשאות גישה וזיהוי ואימות

ממצאים

יצוין כי בדוח 2015, הועלו ליקויים בנושא ניהול ההרשאות וסיסמאות.

המועצה לא ביצעה מיפוי הרשאות, ואינה מקפידה על נהלי הרשאות, תיקוף הרשאות, זיהוי ואימות כנדרש בתקנות. לא קיים ניהול רישום מעודכן של ההרשאות הגישה למאגרי מידע שניתנו לעובדים.

נמצא כי לא קיים נוהל / טופס בקשת הרשאות הכולל את הפרטים הנדרשים; לא בוצע מיפוי לסוגי ההרשאות הנדרשות.

במועצה אין הזדהות חזקה לגישה מרחוק למשתמשי הקצה וגם מנהל מערכות המידע ועובדיו נכנסים למחשבים ולמערכות המידע באמצעות גישה מרחוק פשוטה ואף ללא צורך בסיסמאות חד פעמיות.

מחדלים אלו חושפים את המועצה לסיכונים הכוללים חשיפה לא מורשית למידע.

המלצות

על המועצה לפעול בהתאם לתקנות. כך למשל, יש לקבוע נוהל כאמור לעיל ובו התייחסות נדרשת לתחום ההרשאות; לקבוע הרשאות גישה למאגר לכל עובד במידה הנדרשת לו לצורך ביצוע

תפקידו ולא יותר מזה; יש לבצע מיפוי ורשימת הרשאות ולעדכנה לפי הצורך ובעת שינוי; יש לבטל הרשאות למי שסיים תפקידו – מייד עם סיום התפקיד.

מומלץ לבחון ולקבוע אופן אבטחת גישה מרחוק המתאים לרמת המאגרים.

בד"כ מקובל להמליץ שהזיהוי והאימות יתבססו על אמצעי פיזי הנתון לשליטתו הבלעדית של מורשה הגישה (ביומטרי, כרטיס חכם או Token הנשלח כהודעת SMS לטלפון הנייד). בזיהוי מבוסס שם משתמש וסיסמה יש לקבוע את חוזקה, מספר ניסיונות שגויים ותדירות החלפה. כמו כן, נדרש ניתוק אוטומטי לאחר פרק זמן של אי-פעילות. המלצה זו כפופה להגדרות והתאמות מקצועיות.

מעת לעת ובהתאם לצורך, יש לבחון ולעדכן את רמת ההרשאות לשם צמצום הסיכונים ומניעת נוזקות.

16. חיבור התקנים

ממצאים

במועצה אין הגבלה מספקת בחיבור למערכות שלה באמצעות חיצוניים (כך, מלבד שימוש בהתקנים ניידים קטנים עם USB, ניתן להתחבר ישירות לרשת המועצה כמו שנעשה לעיתים באמצעות מחשבים ניידים בין אם בידי עובדי המועצה ובין אם בידי נותני שירותים או מבקרים). אי הגבלה זו חושפת את המועצה לסיכוני אבטחת מידע. בנוסף לכך, לא בוצע ניתוח של הנושא כנדרש בתקנה 12 לתקנות אבטחת המידע.

המלצות

על המועצה לעמוד בתקנה 12 לגבי חיבור התקנים.

מומלץ להייעוץ בגורם מקצועי.

17. בקרה ותיעוד גישה

ממצאים

המועצה לא מיפתה את נושא התיעוד האוטומטי עבור כל מאגר ולא נקבע נוהל בדיקה לנתוני התיעוד.

מממונה אבטחת המידע נמסר, כי יש מספר מאגרים עם בקרה והגבלת גישה (כגון מאגרים בחברה לאוטומציה, בר טכנולוגיות (ועדה מקומית לתכנון ולבניה) ומערכת מימד – רישום נתוני משרד הפנים עבור התושבים).

לגבי שאר המאגרים, הביקורת מעירה, כי ללא בדיקת התיעוד לא ניתן לדעת האם גורם בלתי מורשה ניגש למאגרים עם מידע רגיש. הדברים מקבלים משנה תוקף במאגרים עם "משתתף משותף" וכך אין אפשרות לדעת על זהות מבצעי הפעולות.

אין ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות של גורמים בלתי מורשים.

המלצות

על המועצה להפעיל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע בהתאם למפורט בתקנה.

מומלץ להגדיר את מנגנון התיעוד ולערוך שינויים ועדכונים בהתאם לצורך.

יש לבצע ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות של גורמים בלתי מורשים.

18. תיעוד של אירועי אבטחה

ממצאים

למועצה אין נהלים לאיתור, תגובה ותרגול של אירועי אבטחת מידע, אין מדיניות בנושא ואין תיעוד. עד מינוי ממונה אבטחת מידע, לא בוצעה בדיקה מסודרת של מרבית אירועי אבטחת המידע. גם כעת, התקציב לא מאפשר ניטור רציף ברמה גבוהה, ולא ניתן לדעת בוודאות שלא היו אירועים כאלה. היה ניסיון לפגיעה במחשבי הוועדה לתכנון ולבניה שהסתיים מהר מאד בזכות ממונה אבטחת המידע ולפי אנשי המחשוב לא התפתח לכדי אירוע.

פורום הנהלה או דרג ניהולי כלשהו לא מקיים דיונים באירועי אבטחה, אין תרגול ואין צוות מקצועי למענה מקצועי לסיכוני ואירועי סייבר.

המלצות

על המועצה לפעול באופן סדור בהתאם לתקנה 11 לתקנות אבטחת המידע בנושא תיעוד אירועי אבטחת מידע, מומלץ לקבוע מדיניות, ליישם טכנולוגיה מתאימה לניטור ואיתור אירועים חריגים ותגובה להם, לקבוע נהלים לאיתור ותגובה לאירועי אבטחת מידע וכן לתרגל.

מומלץ למנות צוות המשכיות והתאוששות מאסון, לקבוע סדר ומדרג פעולות תגובה בהתאם לאירוע האבטחה ולהתפתחותו ולעדכנו בהתאם לצורך.

כעולה מדוח זה, ובהקשר לנדון, מומלץ להיערך מבעוד מועד לאירועי אבטחה שונים ומגוונים ובכלל זה לקבוע מנגנון קבלת התראות, לבצע הדרכות וכו'.

19. עיר חכמה

ממצאים

בשלב זה, המועצה לא החליטה על מעבר ל"עיר חכמה" לפי כל הגדרה שהיא ולא פועלת להטמעת טכנולוגיות מתקדמות חדשות לטובת התושבים.

המלצות

בכל הקשור ל"עיר חכמה" ולהטמעת טכנולוגיות חדשות, מומלץ למועצה לגבש מסקנות והחלטות רק לאחר היוועצות בגורמי מקצוע, לימוד הצורך והכרת ההזדמנויות והסיכונים.

20. מיקור חוץ

ממצאים

נמצא כי במועצה לא נערכה עבודה מקדימה הקשורה לבחינת ההשלכות של שימוש במיקור חוץ לניהול מאגרים עם מאפיינים של הגנת הפרטיות.

נמצא כי המועצה אינה מקפידה על הסכמים עם ספקי שירותי מערכות מידע, אשר מחייב אותם לשמור על הגנת הפרטיות בהתאם לתקנות.

עוד עולה, כי גם כאשר יש בהסכמים סעיפים המחייבים את הספקים במיקור חוץ לאבטח את המידע, המועצה לא נקטה צעדים כדי לוודא או לבקר את עמידת הספק בהתחייבות.

במועצה אין דרישה, פיקוח או בקרה למילוי חובות הספקים כמחזיקי מאגרי מידע. יודגש, כי כאמור, בהתאם לסעיף 17א לחוק הגנת הפרטיות, מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר ; מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

מהחברה לאוטומציה נמסר, כי מדיניות האבטחה שלהם מסודרת ומעוגנת בנהלי אבטחה מסודרים ומתוקננים תחת תקן אבטחת מידע מתקדם ואף העבירה לביקורת מידע בנושא.

בתשובה לשאלת הביקורת, השיבה החברה לאוטומציה כי: "החברה לאוטומציה הינה ספק השירותים למועצה האזורית לכיש, ובפוזיציה זו היא מחויבת לעמוד בדרישות האבטחה של הרשות, ולא להיפך. ובכל זאת, החברה לאוטומציה ממליצה ללקוחותיה, ובהם ספציפית גם בפעילות מול לכיש, לקיים רמת אבטחת מידע הכוללת הגנה על כלל תחנות הקצה, שמירה על נהלי סיסמאות, הגנת וירוסים, בקרת גלישה ומיילים וכד'.

החברה לאוטומציה מפעילה את מערכות המחשוב כאשר נהלים אלה מובנים, והלקוח נדרש להחליף סיסמאות מעת לעת, מסכי המערכת ננעלים לאחר זמן של חוסר שימוש, הלקוח קובע את מרחבי הכתובות מהם ניתן להפעיל את מערכות המחשוב שלו וכד'".

בעניין שאלה על מאגרי המידע, מהחברה לאוטומציה נמסר, כי היא מוגדרת כ"מחזיקת המאגר" והמועצה היא "בעלת המאגר".

הביקורת הפנתה שאלות גם לחברת מילגם המספקת שירותי גביה. להלן חלק מתשובותיה:

"החברה אינה מספקת שירותי מחשוב למועצה. שירותי המחשוב ניתנים למועצה ע"י החברה לאוטומציה. מילגם כן מאפשרת לעובדיה המוצבים במועצה אפשרות שימוש בתוכנה פנימית של מילגם לביצוע פעולות אכיפה כלפי חייבים וכן מערכת המייל. מערכות השייכות למילגם מנוהלות כולן בחוות השרתים של חברת מילגם. עובדי החברה כפופים להנחיות אבטחת המידע של החברה. החברה מנהלת את שכבות האבטחה השונות באמצעות עמידה בתקן מחמיר של אבטחת מידע, כלים טכנולוגיים להגנה מאגרי המידע, הנחיות ומודעות לעובדים ועוד.

בוצעה התעדה מלאה למערכת ניהול אבטחת המידע על ידי מכון התקנים הישראלי אשר מוכיחה שהארגון נוקט באמצעים המתאימים בכדי לממש את מחויבותו לשמירה על המידע ולנהלו בצורה יעילה.... כל מאגרי המידע שמנוהלים בחוות השרתים של מילגם מנוהלים עם דגש נרחב בתחום אבטחת המידע".

החברה השיבה תשובות שליליות לשאלות הביקורת:

האם המועצה הציבה לחברתכם דרישות בתחום אבטחת המידע? ; האם בהסכמים עם המועצה יש דרישה לעמוד בתקני אבטחת מידע ופרטיות? ; האם המועצה בודקת מולכם עמידה בהסכמים בנושא זה?

לשאלת הביקורת, בקשר למאגרי המידע, החברה השיבה שהיא אינה בעלת המאגר ולכן לא צריכה לרושמו.

גם בקשר למוקד המועצה הביקורת לא מצאה מדיניות סדורה, התייחסות בהסכמים ואכיפה כאמור.

המלצות

מומלץ למועצה לקבוע מדיניות בתחום מיקור החוץ, וכמובן עליה לעמוד בכללים.

מומלץ כי המועצה תבחן את סיכוני אבטחת המידע הכרוכים בהתקשרויות.

על המועצה לקבוע בהסכמים עם הגורמים החיצוניים את כל הכללים הנדרשים בהתאם לתקנה 15 ולצורך, ובכלל זה: קביעת מערכות המאגר אליהן רשאי לגשת הספק, סוג הפעולות שהספק רשאי לעשות, המידע שהספק רשאי לעבד, מטרות השימוש, גיבויים, דרך העברת מידע במהלך ההתקשרות, דרך השבת והעברת המידע לידי המועצה בסיום ההתקשרות, כללי אבטחת מידע קונקרטיים, תצהירי סודיות, ועוד כמפורט לעיל.

מלבד האמור לעיל, על המועצה לפרט בנהלים את הנדרש בהתאם לתקנות, ולנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות כנדרש.

כמו כן, מומלץ לפנות לספקי מיקור החוץ ולדרוש מהם הצהרות ואסמכתאות לעמידה בתקנות, לרבות ביצוע מבדקי חדירה, סקרי אבטחה ותעודות תקני אבטחה ולבקרם בהתאם לרמה הנדרשת מכל אחד מהם.

21. מינוי ממונה אבטחת מידע

ממצאים

המועצה מינתה את הבעלים של החברה שמתחזקת את מחשוב המועצה כממונה אבטחה מידע. מינוי זה אינו על פי התקנות, שהרי כך שני התפקידים ותחומי אחריות מרוכזים אצל גורם יחיד באופן אשר מעמידו בניגוד עניינים. על הממונה לפקח על החברה המתחזקת (ומנהל מערכות המידע). מינוי זה הינו בניגוד לתקנה 3(4) לתקנות אבטחת המידע שלפיה: "הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה", אלא שהוסבר שמדובר באישיות נפרדת מהחברה ובמצב זמני.

זאת ועוד, לא הוכנה תוכנית סדורה לבקרה שוטפת.

המלצות

על המועצה למנות ממונה ואחראי אבטחת מידע, שתפקידיו יוגדרו מראש בהתאם לדין ובהתאם לצורך.

מומלץ שממונה ואחראי על אבטחת המידע יהיה כפוף למנכ"ל המועצה או לנושא משרה בכיר אחר, לא ימלא תפקיד נוסף ולא יעמוד במצב של ניגוד עניינים.

מומלץ לבחון ולהחליט בעניין חלוקת העבודה ושיתוף הפעולה בתחום זה עם קב"ט המועצה.

22. מינוי ממונה הגנה על הפרטיות

ממצאים

במועצה לא שמעו על תפקיד ממונה הגנה על הפרטיות. לשאלת הביקורת, מאחר ואין חובה חוקית לכך ואין תקציב עודף, לא מתכוונים למנות בקרוב תפקיד כזה.

המלצות

אכן אין חובה ישירה בחוק למינוי ממונה הגנת הפרטיות ומדובר במינוי וולונטרי, ועדיין לדעת הביקורת, מומלץ למועצה לפעול למינוי כאמור.

זאת לאור החובות בתחום אבטחת המידע והגנת הפרטיות ולאור הסיכונים השונים – משפטיים, תפקודיים ואחרים – העולים מאי הקפדה על הנדרש.

מובן שאין להתעלם מההיבט התקציבי, אך בתור התחלה ניתן למנות עובד קיים ולפעול כך שמינוי זה לא יעמיס מבחינה תקציבית על המועצה. זאת ועוד, תפקיד כזה, עשוי לצמצם סיכונים וגם לחסוך תקציבית.

<u>תיקון ליקויים מדוח 2015</u>

במספר תחומים חלו שיפורים (בעיקר בתחום הגיבוי, חומת האש ואנטי וירוס, רישוי תוכנות, מצלמות מעקב, רישום מאגרי מידע). מחמת הזמן הרב שעבר, פרסום תקנות אבטחת המידע החדשות, עדכוני נהלים והנחיות, חלק מהדברים אינו רלבנטי ולכן אין צורך בבדיקת תיקון כל הליקויים. יש לציין, כי חלק ניכר עדיין רלבנטי וליקויים לא תוקנו באופן מלא בכל התחומים כמפורט לעיל וכפי שבאו לידי ביטוי לאורך דוח זה.

1. בסעיף 130א(א) לצו המועצות האזוריות נקבע, כי על המועצה האזורית לבחור לכל ישוב שבתחום שיפוטה ועדת ביקורת מבין תושביו אשר אינם חברי ועד מקומי, מרשימת תושבים שיציעו את מועמדותם ; מספר חברי ועדת הביקורת לא יפחת משלושה ולא יעלה על חמישה.[37]
2. על ועדת הביקורת לבדוק אם החלטות הוועד המקומי הוצאו לפועל כדין, לבדוק את חשבונות הוועד ולוודא כי פעולותיו נעשו במסגרת תקציבו המאושר וכן לבדוק אם תוקנו ליקויים בפעולות הוועד המקומי אשר נמצאו בביקורות קודמות. [38]
3. לצורך ביצוע תפקידיה, רשאית ועדת הביקורת לקבל מכל חבר ועד מקומי או עובד ועד מקומי, ידיעות, מסמכים והסברים הדרושים לה.[39]
4. מועדים - בתוך שלושה חודשים מתום כל שנה תמציא ועדת הביקורת לוועד המקומי טיוטת דוח ביקורת מפורט שיתייחס לפעילות הוועד המקומי ותאפשר לו להעיר הערות לטיוטה בתוך שלושים ימים ; ועדת הביקורת תקיים דיון בהערות הוועד המקומי ותערוך את דוח הביקורת הסופי.[40]
5. בתוך חמישה חודשים מתום כל שנה, תמציא ועדת הביקורת לידי הוועד המקומי, ראש המועצה ולידי ועדת הביקורת של המועצה את דוח הביקורת הסופי ; דוח הביקורת יהא פתוח לעיון כל תושב בישוב וסיכום תמציתי ממנו יופץ לכל תושבי הישוב בתוך 14 ימים ממועד הגשתו למועצה.[41]
6. חשיבות הוועדה גבוהה מסיבות כלליות של ביקורת על גוף ציבורי ובאופן ייחודי בשל מהות עבודת הוועד המקומי.

ממצאים

7. במשך שנים נציגי הישובים במליאה והוועדים תוזכרו בחובת הוועדים למנות ועדות ביקורת.
8. נציגי הישובים התבקשו להביא שמות מומלצים לתפקיד לאחר בדיקה פנימית (הדברים באו לידי ביטוי בתכתובות ובפרוטוקולים. למשל בפרוטוקול משנת 2014 (24/07/2014): "נציגי המליאה תוזכרו בחובת המועצה למנות ועדת ביקורת לועדים המקומיים בכל ישוב, הנציגים התבקשו להביא מומלצים לתפקיד לאחר בדיקה פנימית בישובים".

37 סעיף 130א(ב).
38 סעיף 130א(ג) לצו.
39 סעיף 130א(ד) לצו.
40 סעיף 130א(ה) לצו.
41 סעיף 130א(ו) לצו.

9. המועצה מינתה חברי ועדת ביקורת לוועדים המקומיים רק ביוני 2016. גם לאחר המינוי, ועדות ביקורת כמעט ולא התכנסו, הוועדים כלל וכלל לא עבדו מול הוועדות, הוועדות לא הגישו דוחות והמועצה מצידה לא ביקשה דוחות.
10. אפשר לקבוע, כי נכון למועד ביקורת קודמת בשנת 2018, ובמשך השנתיים שקדמו לה, ועדות הביקורת חדלו לתפקד לחלוטין.
11. יצוין, כי בסוף שנת 2020 המועצה מינתה חברי ועדת ביקורת בוועדים: ניר חן, אחוזם, כרמי קטיף, בני דקלים, זוהר, שחר, נוגה, שדה משה, נטע, מנוחה, שקף, שדה דוד, יד נתן ותלמים.
12. בביקורת הנוכחית, הביקורת העבירה שאלות למזכירות המועצה בדבר רשימת ועדות הביקורת, דוחות ומסמכים שהתקבלו מאת ועדות הביקורת. נמסר לביקורת כי אין חומר בנושא ולא נמצא מישהו שאחראי על הנושא. רק לאחר התעקשות, הביקורת הופנתה לפרוטוקול האמור מסוף שנת 2020.
13. לאור האמור, הביקורת הנוכחית הינה גם כבדיקת תיקון ליקויים.
14. הביקורת הפנתה מכתבי שאלות לוועדים המקומיים. חלק השיבו שאין להם ועדת ביקורת והרוב לא השיבו. חלק מסרו שמות של ועדת ביקורת של האגודה השיתופית. בהקשר לכך יצוין, כי גם רישום המועצה (בהסתמך על הפרוטוקול האמור מסוף שנת 2020) לא נכון, שכן הוא אינו מעודכן. כך למשל, שמות חברי ועדת ביקורת הרשומים בו לכרמי קטיף היו של האגודה ולוועד מונו אחרים לפי פרוטוקול המועצה מתאריך 30/12/2021. לפי הדיווחים שנמסרו לביקורת מנציגי הוועדים עולה כי ועדות ביקורת אינן מתפקדות וכי לא העבירו דבר למועצה.
15. מהביקורת עולה, כי הגם שהמועצה מינתה חברי ועדות ביקורת, ולפי הפרוטוקולים הנזכרים אין לכל הוועדים (עוצם, נהורה, אליאב ואמציה), הרי אין כל תפקוד של הוועדות ולא נראה שהמועצה פועלת לשם כך.

המלצות

16. המועצה היא הרובד העליון בניהול המקומי במועצה האזורית לכיש. המועצה האצילה סמכויות לוועדים המקומיים לצורך אספקת שירותים במגוון תחומים בממשק ישיר לחיי התושבים כחינוך ותרבות, בריאות, רווחת קהילה, גינון ושיפור פני הישוב, פיתוח פיסי וחברתי, ביטחון אישי ותחזוקת מתקני משחקים ושטחי ציבור אחרים.
17. הוועד המקומי אחראי לניהול היישוב, ומחובתו לשרת את התושבים באופן מסודר, שוטף, רציף ועקבי. בין היתר, על הוועד להסדיר את נושא החשבונות הכספיים כולל חשבון בנק, החזקת כספים, ביקורת והגשת דוחות כדת וכדין; העסקת עובדים כדין; לקיים ישיבות כנדרש, לוודא נוכחות חברים בישיבות, לוודא פקיעת חברות של חברים שלא נכחו כנדרש, לנהל פרוטוקול ולפרסמו לתושבים ועוד.

18. ועדת ביקורת הינה ועדת חובה שעליה לתפקד ולפעול בהתאם להוראות הדין; הביקורת ממליצה לוועד המקומי ולמועצה לוודא את קיום הביקורת ולהציע הדרכה לשם ביקורת מקצועית ולפי חוק.
19. על ועדות הביקורת לתפקד ולפעול בהתאם להוראות הדין.
20. מומלץ לוועדות לקבל הדרכה. הביקורת מציעה את עזרתה בהדרכה.
21. הביקורת מפנה את המועצה לבדק בית, שכן היא הרובד העליון של השלטון המקומי, ועליה לדאוג לרווחת התושבים ולהענקת השירותים המוניציפאליים.
22. הביקורת מדגישה, כי המועצה שהינה הרובד העליון בניהול המקומי כאמור, איננה יכולה להתנער מאחריותה ולטעון: "האצלנו סמכויות לוועדים!". עליה לבקר, לפקח, להדריך ובמקרה הצורך ליטול סמכויות חזרה ולפעול.
23. הביקורת ממליצה למועצה לוודא מי חברי ועדות הביקורת, להכין רשימה מסודרת ובמידת הצורך למנות חברים חדשים ולבקש קבלת דוחות.
24. הביקורת קוראת וממליצה למועצה להדריך את הוועדים המקומיים ואת ועדות הביקורת בתחום הנדון, ולהביא בפניהם את הוראות הדין, הנחיות וכללים לעבודה חוקית, נכונה ויעילה.

תיקון ליקויים מדוחות קודמים

ליקויים ותיקונם נדונו לעיל הן בתחום אבטחת המידע והן בתחום ועדות הביקורת.

הסעות תלמידים

תחום ההסעות במוא"ז לכיש זכה בשנים האחרונות ובזמן האחרון להתייחסויות שונות כמו פניות הורים למועצה, ביקורת במועצה וביקורת המדינה. לפני סגירת הדוח נערכה הפגנת הורים קטנה בנהורה ו"שביתה" בדמות אי שליחת מאות תלמידים לבית ספר כאות מחאה בנושא איחורים, לכלוך באוטובוסים, שפה לא יפה של נהגים והימשכות זמן ההסעות. לביקורת לא נמסרו נתונים מדויקים, אלא בשיחות בע"פ.

בדוח הביקורת לשנת 2018 נבדקו מספר היבטים בתחום ההסעות.

במחצית השנייה של שנת 2020 בדק משרד מבקר המדינה היבטים בנושא הסעות תלמידים למוסדות החינוך הרגיל ולמוסדות החינוך המיוחד ברשויות המקומיות – גם במוא"ז לכיש.[42]

בשנת 2021 נבדק תחום ההסעות בעיקר על רקע ביקורת המדינה ובדוח זה נבדק תחום תיקון הליקויים.

בדיקת נכונות שיעורי השתתפות

בדוח המבקר נכתב כי, "בביקורת נמצא כי שיעור ההשתתפות של משרד החינוך בהסעת התלמידים של המועצה האזורית **לכיש** הסתכמו בשנים 2018 ו-2019 ב-65% וב-55% מהעלות בפועל, זאת למול שיעורי ההשתתפות שקבע לה משרד החינוך (85%). גזבר המועצה מסר במהלך הביקורת כי הדבר עלול לנבוע מכך שהמועצה האזורית **לכיש** כללה בהוצאות חברות ההסעות המסיעות את התלמידים בחינוך המיוחד גם את ההוצאות עבור מלווי התלמידים[43]. עלה כי המועצה לא וידאה שמשרד החינוך העביר לה את מלוא סכומי ההשתתפות שהיה עליו להעביר".

בתשובה לממצאים אלו מגזברות המועצה נמסר, שלאחר בדיקה נוספת התברר כי אחוז ההשתתפות של משרד החינוך גבוה יותר והינו תקין.

מבדיקה חוזרת של הביקורת מול מנהל מחלקת ההסעות (גם לאחר תלונה בדבר אי תקצוב הסעות לשומריה) עולה, לדברי מנהל מחלקת ההסעות, כי המועצה קיבלה את מירב ההקצבה ממשרד החינוך. הדברים נתמכו במספר מסמכים שהציג מנהל מחלקת ההסעות. מהגזברות נמסר כי נערכה בדיקה והדברים הועברו למבקר המדינה.

מנהל מחלקת ההסעות הוסיף שגם שמשרד החינוך העביר את סכומי ההשתתפות, "המועצה מוציאה הרבה יותר ממה שמקבלת". הסבר מנהל המחלקה היה שהפער נובע בעיקר בשל הסעות החינוך המיוחד וניסיונותיו להוסיף הסעות כדי למנוע ולצמצם עיכובים.

42 מדובר בדוח על הביקורת בשלטון המקומי, התשפ"א-2021. הנתונים והציטוט הערוך או המובא כמקורו שלהלן הינו מתוך דוח זה (להלן: "דוח מבקר המדינה").

43 המועצה אמורה לבצע רישום נפרד בעבור הוצאות מלווי ההסעות, שבעבורן מגיעה לה השתתפות נוספת.

לדעת הביקורת, על העובדות בדבר נכונות שיעורי ההשתתפות של משרד החינוך להיות ברורות וידועות ועם סיכום ברור גם במהלך העניינים השוטף ולא רק בבדיקה בתגובה לשאלות הביקורת.

איחוד מסלולים והתייעלות

משרד מבקר המדינה העיר לעניין נחיצות פרטי מידע להתייעלות, כמו מספר התלמידים המוסעים ומרחק הנסיעה בכל אחד מהמסלולים שהן מפעילות. פרטי המידע האלה יאפשרו לייעל את מערך ההסעות, לבדוק את ההיתכנות לקיצור משך הנסיעה ואת איחוד המסלולים. לדעת מנהל המחלקה, גם אם חסרו פרטים עדיין הם עובדים באופן יעיל. ובכל אופן, בעקבות הביקורת, תחום המסלולים נבחן ואכן כיום מתבצעים שילובים נוספים.

מבקר המדינה הוסיף והעיר, כי מומלץ שהמועצה האזורית לכיש, ושאר הרשויות המקומיות, יבחנו מפעם לפעם את האפשרות לאיחוד מסלולי הסעה בתחום שיפוטן ולשיתוף מסלולי הסעה עם רשויות מקומיות סמוכות. כמו כן, מומלץ למועצה לבחון מול משרד התחבורה תוספת קווים לתחבורה ציבורית.

לדעת הביקורת, רק נתונים מדויקים יכולים לתת תמונה מדויקת ולדעת האם עובדים באופן יעיל – גם כלכלי, ולכן ההמלצה הייתה להתחיל בעבודה – גם בתחום זה - באופן ממוחשב וסדור.

ממחלקת התחבורה נמסר כי הדברים היום ממוחשבים בחלקם ועובדים על שיפורים שיאפשרו ניהול ממוחשב רחב יותר.

לדברי מנהל מחלקת התחבורה, התוכנה שודרגה וכיום כל המסלולים ממוחשבים.

מנגנון הקנסות

בדוח מבקר המדינה עלה, כי המועצה האזורית לכיש לא דרשה פיצויים מוסכמים בשנת 2018 וכי בשנת 2019 דרשה 800 ₪ והביקורת בשנת 2021 מצאה שאכן בשנים האחרונות המועצה כמעט ולא דרשה פיצויים מוסכמים (קנסות) מקבלני ההסעות שלא עמדו בתנאי חוזה ההסעות. זאת על אף העובדה שבמשך השנים הגיעו פניות רבות מהורים ומבתי ספר שונים על חלק מקבלני ההסעות ועל הנהגים על איחורים, התנהגות בלתי נאותה של נהגים כולל עישון ועוד; ועל אף העובדה שהמועצה העירה במספר מקרים לחברות ההסעה על ליקויים שונים ועל אף העובדה שמשכ"ל העירה על מספר תקלות.

בביקורת 2021 מנהל המחלקה חזר והסביר שגם שניתן להטיל קנסות לפי ההסכם, לא תמיד נכון וחכם לעשות זאת, ויש לשמור על קשר טוב עם חברות ההסעות שלעיתים נדרשים לתגבר ולסייע בעת אירועים לא צפויים או לערוך שינויים לא מתוכננים.

עם זאת, התקיימה פגישה עם זכייני המועצה והובהרה להם חשיבות העמידה בהסכמים והסנקציה שבהפרה.

בביקורת זו, מנהל מחלקת התחבורה הציג כמות גדולה יותר של קנסות.

הביקורת חוזרת על המלצתה, שעל המועצה לראות בסעיפי הפיקוח והפיצויים ככלי ליעילות ולבטיחות ההסעות. במקרים המתאימים יש לבחון ואף לדרוש תשלום פיצוי על הפרות.

מומלץ לרכז, לתעד ולנתח את ההפרות, לבחון תיקון ליקויים ולהסיק מסקנות.

נתוני התלמידים

בביקורת הקודמת חלק מהנתונים בדבר מספרי התלמידים המוסעים ושמותיהם, לא היו זמינים ומעודכנים במערכות המועצה. בביקורת חוזרת נמצא תיקון חלקי לנושא – במיוחד שאספו נתונים לצורך הגשה למבקר המדינה. מבחינת נתוני רכבי ההסעות, הרי הם מעודכנים במערכת כולל GPS כך שניתן לדעת בכל רגע נתון היכן נמצא כל רכב. בביקורת לשנת 2021 בשיפור מהדוח הקודם, נמסר כי נעשה שימוש רחב יותר במערכת הממוחשבת לניהול ההסעות, אם כי עדיין לא לכלל רכבי ההסעה. מערכת זו מספקת בזמן אמת נתונים על מיקום ההסעה בכל זמן וכך ניתן לדעת זמני הגעה, נסיעה במסלול הנכון, הגעה בזמן או איחור וכו'.

בביקורת הנוכחית עולה כי אין נתונים בדבר שמות התלמידים. לדברי מנהל מחלקת התחבורה, בשלב זה הוא לא יכול לעמוד בכך.

לדברי מנהל מחלקת ההסעות ולפי תכתובות שהציג לביקורת,44 יש הערכה סבירה שעד ינואר 2023 כל האוטובוסים והמסלולים יהיו מנותרים.

המלצות

הביקורת קוראת לעבוד בהתאם להמלצות מבקר המדינה, כי המוא"ז לכיש ועוד רשויות, ינהלו רישום מסודר בו יפורטו בכתב מספר התלמידים המוסעים ומרחק הנסיעה בכל אחד מהמסלולים שהן מפעילות. פרטי המידע האלה יאפשרו לייעל את מערך ההסעות, לבדוק את ההיתכנות לקיצור משך הנסיעה ואת איחוד המסלולים.

הביקורת חוזרת על המלצתה לקבוע בנוהל כאמור להלן - דרישה מבתי הספר להעברת נתונים מעודכנים ולנהלם ולעדכנם במערכת על בסיס קבוע.

---

44 למשל מתחום ההיסעים במשכל לקבלנים: "בהמשך לדרישת **מ.א לכיש**,
הנכם מתבקשים לנטר את כל המסלולים המבוצעים על ידכם, לרבות קבלני המשנה, באמצעות מערכת 'טרפיקל' (מערכת לניהול מערך היסעים ברשויות).
מדובר על אותו תהליך שמתבצע ברשויות העובדות עם מערכת טרפיקל.
אפשרויות ההתחברות למערכת (צד קבלן של 'טרפיקל' / ממשק YIT),
אפשרויות הניטור (אפליקציית נהג / ממשק ל GPS של הרכב).
וכן הדרישה לעדכן את המערכת באופן שוטף ויומיומי בהתאם לשינויים והעדכונים.
מצ"ב מכתב עם הסבר מפורט על מערכת 'טרפיקל' ואפשרויות ההתחברות.
לתיאום הדרכה במידת הצורך, שאלות ופרטים נוספים ניתן לפנות...".

הביקורת ממליצה ליישם מוקדם ככל האפשר את מערכת ניתור רכבי ההסעה על כלל רכבי ההסעה.

הביקורת חוזרת על המלצתה לבצע איסוף נתונים קבוע לפי פילוחים שונים ובהתאם לכך לקיים ניתוחים שוטפים הכוללים בקרות שונות, מלבד משכ"ל, ובהמשך לכך להפיק לקחים בתחומים הנדרשים.

נהלים

בדוח הקודם צוין, כי אין כללים ונהלים כתובים הקובעים את סמכויות בעלי התפקידים, זכאויות להסעות ולמלווים, בדיקת עמידה בהסכמים, הטיפול בפניות הורים, נהגים ומורים, הבקרה והפיקוח בשטח על חברות ההסעה, על הרכבים, על הנהגים, על המלווים, על הבטיחות וכו'.

ליקוי זה לא תוקן והביקורת חוזרת על המלצתה, שעל המחלקה והמועצה להתקין כללים ונהלים בתחום הסעות התלמידים.

הנחיות ונהלים יסייעו למחלקת התחבורה ולמועצה לשם יישום התהליכים באופן ראוי וביצוע בקרות, יסייעו לתושבים ויגבירו את אמונם ברשות.

הביקורת ממליצה שההנחיות והנהלים ייערכו בהליך נכון הלוקח בחשבון מדיניות ומעשה. בתחום המדיניות: הליך שיטלו בו חלק ראש המועצה והמליאה. בשאר התחומים: המנכ"ל, הגזבר ומנהל המחלקה, תוך שיתוף המחלקות הרלבנטיות.

הנהלים יכללו, בין היתר, תהליכי עבודה נכונים, קביעת בעלי תפקידים וסמכויותיהם, תהליכי עבודה, בקרה ועוד.

הסכמים

בדוח הקודם – נמצאו חוסרים בהסכמים.

גם למבקר המדינה נמסר ממשכ"ל, כי בחוזי ההתקשרות שנחתמו במסגרת המכרזים שהיא פרסמה בשנים 2018 ו-2019 נדרשו הקבלנים להמציא לרשויות המקומיות את המסמכים (כגון רישיונות רכב וביטוחים בתוקף ומסמכים המעידים כי ברכבי ההסעות מותקנות המערכות הטכנולוגיות המתאימות), ואולם בבדיקת משרד מבקר המדינה הועלה כי למועצה האזורית לא הייתה נגישות לתיקים שבהם רוכזו מסמכי חברות ההסעות.

ממצאים מדוח מבקר המדינה: "המועצה האזורית **לכיש** התקשרה לקבלת שירותי הסעות תלמידים עם תשע חברות הסעות זכייניות משכ"ל, מרשימת זכייני המכרז שפרסמה משכ"ל.

בתיקי חברות ההסעה שנוהלו במועצה לא נמצאו בעת הבדיקה בנובמבר 2020 מסמכים בסיסיים רבים, בניגוד לחוזים שנחתמו עם חברות ההסעה אשר בהם נקבע כי בתוך כמה

ימים מיום חתימתם יוגשו למועצה כל המסמכים המפורטים בנספח לחוזה, לרבות המסמכים הקשורים לקבלני משנה, אם אושרה העסקתם,[45] כלהלן:

שום חברה לא המציאה אישור על כשירות רפואית של הנהגים, אף כי חמש חברות הצהירו על כשירות הנהגים; רשימת כלי הרכב שבהם יבוצעו ההסעות לא נכללה בתיקיהן של שש חברות; חברה אחת לא צירפה רישיונות רכב וחמש חברות אחרות המציאו רישיונות רכב שמרביתם נמצאו לא עדכניים[46]; שתי חברות לא המציאו ביטוחי רכב, וארבע חברות אחרות המציאו ביטוחי רכב שרובם נמצאו לא עדכניים[47]; שתי חברות לא המציאו ההיתר ברישיון הנהיגה להסיע קבוצת ילדים; שתי חברות לא המציאו רישיונות נהיגה של נהגים; שלוש חברות לא דיווחו כי הותקן בכלי הרכב שבבעלותן חיישן המתריע על ילדים שנשכחו ברכב; שש חברות לא דיווחו כי הנהגים השתתפו בהשתלמות בשנה האחרונה; שתי חברות אחרות דיווחו כי ההשתלמות האחרונה שנהגיה השתתפו בה התקיימה בשנת 2019, וחברה אחת דיווחה כי ההשתלמות האחרונה בנושא התקיימה בשנת 2018, רק שלושה מתוך 13 נהגים השתתפו בה; שש חברות לא המציאו את רשימת כלי הרכב שיעמידו לרשות המועצה בעת חירום; שש מהחברות לא המציאו רשימת נהגים; לא נמצאו מסמכים שיעידו כי בכלי הרכב של שלוש חברות הסעות הותקנה מערכת לניהול צי רכב. מסמכים עדכניים בסיסיים נוספים חסרו אף הם.

בעקבות הביקורת העבירה המועצה לצוות הביקורת את מרבית המסמכים החסרים, ואולם מסמכי רישיון של כלי רכב וביטוח חובה של שלוש חברות היסעים לא הומצאו; 20 רישיונות רכב שהמציאה אחת מחברות ההיסעים נמצאו לא עדכניים; 10 ביטוחי כלי רכב של חברה שנייה נמצאו לא עדכניים (תוקפם פג בסוף שנת 2019) ושניים מתוך 24 ביטוחי חובה של חברה שלישית היו מעודכנים".

בביקורת חוזרת נבדק מדגם מההסכמים עם חברות ההסעה ונמצאו כל המסמכים הנדרשים.

45 בנספח לחוזים נקבע כי יוגשו המסמכים האלה: כתב מינוי של קצין הבטיחות בחברת ההסעות, כתב הסמכה בתוקף, רישיון הפעלה למשרד הסעות, אישור קיום ביטוחים תקף, רישיון ניהול עסק תקף; רשימת כלי הרכב שיופעלו (לרבות כלי רכב של קבלני משנה), הצהרה חתומה על ידי קצין הבטיחות של הקבלן כי כלי הרכב האלה כשירים ומותאמים להסעת תלמידים ויש בהם מערכת לניהול צי רכב, העתקי רישיונות הפעלה של כלי הרכב, העתקי רישיונות כלי הרכב, רישום ברישיונות "היתר הסעת תלמידים", העתקי תעודות ביטוח חובה של כלי הרכב, אסמכתאות בדבר התקנתן של מערכות ומתקנים בכלי הרכב בהתאם לדרישות הרשות המזמינה בנוהל הצעת המחיר וכנדרש בחוזה ההתקשרות, כגון מערכת התרעה נגד שכחת ילדים וכן רשימת כלי הרכב שיוכל הקבלן להפעיל למתן שירותי הסעות במצב חירום; רשימת הנהגים מבצעי ההסעות והצהרה חתומה על ידי קצין הבטיחות של חברת ההסעה כי הנהגים מורשים להסעת תלמידים והם בעלי ניסיון של שנתיים בהסעת תלמידים, אישור רפואי על מצב בריאות תקין של כל נהג, אישור משטרה על היעדר עבירות מין, העתקי רישיונות נהיגה של הנהגים ברישיון היתר הסעת תלמידים, אישור קצין הבטיחות של חברת ההסעה שהנהגים עברו בשנה האחרונה השתלמות בטיחות ובה הובהרו כל התקנות הנוגעות לנושא הסעת תלמידים (חוזר מנכ"ל משרד החינוך, תקנות התעבורה והנחיות משרד הרווחה).

46 לדוגמה, 47 (מ-67) רישיונות הרכב שהמציאה אחת החברות לא היו עדכניים: ל-17 מהם פג תוקף הרישיון בחודשים אוגוסט עד דצמבר 2019, ותוקף הרישיון של 24 אחרים פג בחודשים ינואר עד מאי 2020.

47 לדוגמה, נמצא כי פג תוקפם של 53 (מכלל 91) ביטוחי הרכב שהמציאה אחת החברות (לגבי 31 פג התוקף בסוף שנת 2019, ולגבי 22 אחרים התוקף פג בחודשים פברואר עד מאי 2020).

לדברי מנהל מחלקת התחבורה, עד ינואר 2023 כל המסמכים יהיו מרוכזים במערכת ממוחשבת במשכ"ל וניתן יהיה לצפות בכולם.

תחום הליווי בחינוך המיוחד

מבקר המדינה הגיע לממצאים הבאים: "בשנות הלימודים התשע"ח - התש"פ הועסקו 16 - 19 מלוות בהסעות החינוך המיוחד במועצה האזורית **לכיש**: המועצה העסיקה ישירות ארבע או חמש מהן, וחברות ההסעה העסיקו ישירות את שאר המלוות (11 - 14). אחת העובדות מועסקת 8 - 9 שעות ביום, ושאר המלוות מועסקות 3 - 5 שעות בממוצע ליום.

בידי המועצה האזורית **לכיש** אין פרטים על המלוות, הן אלו שהיא העסיקה והן אלו שחברות ההסעה שהעסיקה ישירות, באיזה אופן התקבלו לתפקיד, מהי רמת השכלתן, מהן כישוריהן מרי רמת מסוגלותן לעבודה עם ילדים ואילו הכשרות עברו לצורך מילוי התפקיד וכו'. המועצה לא קיימה הדרכה המיועדות לכלל המלוות בשלוש השנים האחרונות.

המועצה מסרה בעניין זה כי באחריות הקבלן לבצע את ההדרכות למלוות".

הביקורת מפנה לדוח הביקורת בעניין זה, שעסק בנושאים הבאים:

- **פיקוח בטיחות בהסעות תלמידי החינוך המיוחד.**
- **הביקורת המליצה** למועצה להתמודד עם הבעיות ולעשות מה שבידיה, כגון הגדרה ברורה יותר של תפקידי המלווה, סמכויותיו וחובותיו, באופן כללי ובהסעות ספציפיות תוך התייעצות עם אנשי מקצוע במועצה ולאור מגבלות הילדים המוסעים; על המועצה לוודא קיום תיקי עובד הכוללים את כל האישורים הנדרשים וכן הסכמי העסקה מסודרים הכוללים את הגדרות התפקיד; יש לדאוג להדרכות ולהשתלמויות מסודרות לכל המלווים, לוודא שהמלווים יתחילו בתפקידם רק לאחר קיום השתלמות כללית, ושכל מלווה מקבל את הדרכה מיוחדת ומתאימה לליווי הספציפי ובכלל זה מודעות לכל הנדרש כולל בעיות ופתרונן, ודרכי התקשרות עם הורים והצוות החינוכי; הביקורת המליצה שמפגשי ההדרכה הכלליים עם המלווים יכללו את כל ההדרכה הנדרשת לביצוע הליווי כראוי. כמו כן, מומלץ שההדרכה תכלול מפגש והדרכה של גורמים רלבנטיים. מפגש כזה יהווה תנאי חובה בטרם כניסה לעבודה ומומלץ להחתים את המלווים על "טופס ההנחיות" כנספח לחוזה; ניתן לקבוע נהלים שיקבעו את חובת המלווה לדווח לצוות החינוכי של התלמיד ו/או להוריו על התנהלותו בהסעה ולדרוש מן המלווה לחתום על טופס שמירת סודיות; מומלץ גם להכין רשימת מלווים לגיבוי.

הביקורת מפנה לדוח הביקורת בו עסקה גם במענה לפניות הורים לילדי החינוך המיוחד; חיסכון בתחום ההסעות והליווי; איחוד קווים ושיקולי חיסכון; אפליקציית עדכון ליווי; חשיבות ההסעות והליווי בהיבט הרגשי והחינוכי – חלק מהשער לפתיחה ולסיום יום הלימודים.

יצויין, כי לאחר העברת הממצאים ממבקר המדינה, הורחבה משרה של עובדת, שעבדה בחצי משרה, למשרה מלאה והיא מסייעת למנהל המחלקה ומתמקדת בחינוך המיוחד.

מנהל מחלקת התחבורה הציג רשימת מלוות. כל המלוות מקבלות תדרוך באמצעות קבלני משכ״ל.

המלצות

המלצות הביקורת מתאימות גם לאחר בדיקה נוספת ויש לחזור על הדברים, שעל אף שהמועצה משקיעה זמן ומשאבים בתחום הסעות תלמידי החינוך המיוחד, עליה לבחון היטב את התחום על כל היבטיו ולשפר מה שניתן. בין היתר, מדובר בנושאים הבאים:

א. דרך ותנאי ההתקשרות עם חברות ההסעה;
ב. התאמת הנהגים, רישוי, עמידה בתנאים ואישיות מתאימה;
ג. הדרכה במעגלים השונים: הורים, תלמידים, חברות ההסעה, נהגים, מלווים, בתי הספר מנהלים ומורים;
ד. התאמת הרכב ועמידתו בדרישות הדין, משרד התחבורה וחוזר מנכ״ל;
ה. ציוד ואבזור;
ו. גישה בטוחה ונגישות מתאימה לתחנה ולרכב ההסעה;
ז. בקרה, פיקוח ובדיקה של אירועים חריגים והפקת לקחים;
ח. בחירת המלווים, העסקתם והדרכתם;
ט. מסלול הנסיעה, משך הנסיעה, איחוד קווים;
י. בדיקה, התאמה ותקינות תחנת ההעלאה וההורדה;
יא. הרגישות הנדרשת, הקשר עם ההורים ובכלל זה ״כתובת״ במועצה לפניות הורים בתחום, הדרכה והסבר על חובת ההמתנה להסעה עם אדם מבוגר וכן בזמן קליטת התלמיד מהסעת האיסוף.
יב. מקרים מיוחדים שלא מתוקצבים בידי משרד החינוך או משרד הרווחה.

הנה כי כן, בהסעות תלמידי החינוך המיוחד, יש לתת את הדעת על העובדה כי ההסעה הינה חלק מהשער לתחילת היום בבית הספר וחלק משער הסוגר את יום הלימודים.

לעיתים קיימים קשיי הסתגלות במעבר בין הבית לבית הספר, לעיתים זמני הנסיעה ארוכים, לעיתים נדרש יחס ״רגיל״ ולעיתים התייחסות ״מיוחדת״, יש גם מצבים של כאבים וסבל שלא נשמעים.

קשת המקרים רחבה מאד, אין פתרון אחד המתאים לכל התלמידים, ולעיתים נדרשת גמישות גם באשר לתלמיד בודד. מה שברור, שנדרשים תשומת לב ורגישות לתלמידים שכל אחת ואחד מהם ״עולם מלא״.

הנהגים והמלווים הינם הקרובים ביותר לילדים לפני הכניסה למוסדות החינוך ועליהם להיות בעלי ניסיון, מקצועיים, אחראים, ובעלי אישיות מתאימה להסעת תלמידים.

על כל הגורמים המעורבים ובמיוחד על המועצה כגורם מתכלל וראשי בניהול וארגון תחום ההסעות להיות ערים לנושא ועם מלוא תשומת הלב למכלול ההיבטים הנדרשים לטובת התלמידים.

מומלץ להגדיר תפקידים ולפרטם ביחס לתחום זה.

ממצאים

לצורך בחינת ציוד האוטובוסים והתנהלותם בפועל, התבקשה המחלקה לספק דוחות בדיקה שערכה ברכבי ההסעה. לא היו בדיקות של המועצה עצמה, אלא של משכ"ל. גם בביקורת הנוכחית לא היו בדיקות של המועצה.

בדוח מבקר המדינה עלו ליקויים של פחות בדיקות בטיחות מהנדרש ממשכ"ל ושנדרשת הכנת תוכנית ביקורת שנתית ומעקב אחר יישומה.

ההמלצה בדוח ביקורת לשנת 2021 הייתה, בין היתר, לדרוש ממשכ"ל יותר בדיקות בטיחות באופן יזום ומפתיע. הביקורת הוסיפה, כי ראוי לבצע בקרות נוספות מטעמה ולוודא שבקרת משכ"ל מתבצעת כראוי.

מבקר המדינה המליץ למועצה האזורית לכיש להכין תוכנית ביקורת שנתית לביצוע בקרה על מערך ההסעות ותעקוב אחר מימושה, וכן לוודא שמשכ"ל תבצע היקף של ביקורות שנתיות, כפי התחייבותה.

מנהל המחלקה מסר, כי תוכנית הביקורת היא של משכ"ל והיא מבוצעת בידיהם. מנהל המחלקה הציג לביקורת דוגמאות רבות ובכלל זה תמונות מבקרות שונות מהחודשים האחרונים יוני – נוב' 2022.

אין למועצה תוכנית שנתית מנותקת ממשכ"ל.

בדוח הביקורת משנת 2021 הורחב בעניין ההמלצות ובשל חשיבות הדברים, הביקורת חוזרת על עיקרי הדברים:

1. על מנת לתגבר את הפיקוח והבקרה, הביקורת קראה וקוראת למועצה לבצע פיקוח ובקרה באופן יזום, מתוכנן, שיטתי והדוק לבחינת קיום הוראות הבטיחות בעניין הסעת תלמידים בכל סוגי הרכבים ובכל סוגי ההתקשרויות. גם כשאין תקציב גדול לצורך העניין, ניתן וכדאי לבצע ביקורות פתע ולדרוש קיום ביקורת רחבה והדוקה יותר ממשכ"ל. במקביל, יש לבחון את הנושא התקציבי ומסגרת התפקיד המיועדת לעניין.
2. ברור כי מינוי מנהל מטה בטיחות כמובא בחוזר מנכ"ל משרד הפנים וקצין בטיחות, היה בו לקדם את התחום הבטיחותי, אך ניתן לעשות רבות גם במסגרת רצון המועצה שלא להרבות בתפקידים לצורכי חיסכון.
3. לדעת הביקורת, במסגרת זו, ועד מינוי ממונה בטיחות, על המועצה להגדיר את תפקיד מנהל מחלקת התחבורה כתפקיד מתכלל ואחראי, בין היתר, לפיקוח על קיום דרישות הבטיחות בהסעות תלמידים כמתחייב מחוזר המנכ"ל. מן הראוי כי במסגרת הגדרת תפקידו של מנהל מחלקת התחבורה, תוגדר אחריותו גם בנוגע

לפיקוח ובקרה על הסעות התלמידים באמצעות קבלני ההסעות. מובן כי בהקשר זה ייתכן וראוי לבחון השמת מי מעובדי המועצה לצורך בקרה ופיקוח מקצועי בשטח, ככל שיש אדם מתאים מקצועי לכך או שיוכשר לכך.

4. לדעת הביקורת, על המועצה לקבוע באופן ברור ומוגדר את תפקיד ממונה בטיחות ההסעות, סמכותו ואחריותו. בין היתר, יש להבטיח את רמת הבטיחות הראויה הן בכל הקשור לתפקידים הרלבנטיים בבתי הספר וברור שמול חברות ההסעה, קציני הבטיחות, הנהגים המלווים וכל הגורמים הרלבנטיים. לדעת הביקורת, על ממונה הבטיחות לפעול מול בתי הספר. בין היתר, ניתן לדון עם מנהלי בתי הספר על הפעולות הנדרשות והאפשריות לשם עמידה ברמה ראויה של בטיחות.

5. כך, ועל בסיס ההוראות בחוזר המנכ"ל, ראוי לקבוע נוהל דיווח של בתי הספר בדבר פעולותיהם כגון:

א. ייזום פעולות חינוך והסברה במהלך השנה;

ב. מינוי רכזי ונאמני הסעות;

ג. הדרכה ושיתוף ההורים לשם הדרכה והנחיה בכל הנוגע לאחריותם הישירה להתנהגות הילדים בתחנת האיסוף וההורדה, בזמן הנסיעה בחציית כביש וכדומה;

ד. בדיקת אירועים חריגים והפקת לקחים;

ה. הדרכת תלמידים; בדיקה לגבי היעדרות תלמידים;

ו. "קיום מורה תורן" שבין היתר יוודא עלייה בטוחה להסעה, איסור מעבר מאחורי רכב ההסעה ומלפניו, סיוע לילדים בזמן העומס וההמולה בתחנות ההסעה ושמירה על סדר ועל התנהגות נאותה בתחנות ההסעה.

6. אכן חלק מההוראות המופיעות בחוזר מנכ"ל, מופנות לבתי הספר, אך לדעת הביקורת, על הרשות המקומית ללמוד אותן היטב, לשאוב מהן את ההנחיות הקשורות אליה ולפעול בשיתוף בית הספר למען בטיחות התלמידים.

7. לדעת הביקורת ובהמשך לאמור לעיל בדבר הצורך ב"תפקיד מתכלל", המצב הקיים בו אין למועצה ממונה בטיחות בתצורה כלשהי (מנהל מטה בטיחות / קצין בטיחות) אינו תקין. על המועצה למנות אדם לתפקיד של מנהל מטה הבטיחות כמובא בחוזר מנכ"ל משרד הפנים או לקבוע כי עד אז למנהל מחלקת התחבורה, לאחר הכשרתו לנושא, אחריות כוללת גם על הבטיחות ובין היתר:[48]

א. אפיון צרכי הבטיחות בהכנת מכרזים לבחירת קבלני משנה בתחום ההסעות.

48 מתוך תפקידי קצין בטיחות ברשות המקומית לפי הגדרות משרד הפנים.

ב. הוצאת מכתב תקופתי לקבלת אישור תקינות ובטיחות של כלי הרכב מקציו הבטיחות של קבלן המשנה.
ג. פיקוח על תקפות האישורים של נהגי קבלני המשנה, כפי שהתקבלו מקציני הבטיחות של חברות קבלני המשנה.
ד. בדיקת תקפות רישיונות כלי הרכב של קבלני המשנה.
ה. הפעלת סנקציות כלפי קבלני המשנה אם חרגו מהתנאים שנקבעו במכרז, או עברו עבירות תנועה – לרבות עצירת חשבונות שהוגשו לתשלום.
ו. יש להגדיר היטב תפקידים ולהחליט על תפקיד מנהל המחלקה – בנוסף לתפקיד לממונה ישיר ממחלקת הנדסה - באשר למיפוי כל תחנות האיסוף וההורדה של הילדים ברשות המקומית ובדיקה שתחנות אלו מאפשרות גישה בטוחה לרכב ההסעה, ללא הפרעה לתנועה הזורמת, וכן שהורדת הילדים תתבצע בצד שבו נמצא מוסד החינוך ובצד שבו נמצא ביתו של התלמיד.
ז. תדרוך חברות ההסעה והנהגים שלהן בנושאים הנוגעים לבטיחות בהסעות.
ח. תחקור כל אירוע חריג במהלך ההסעות על פי כללים שייקבעו מראש בידי המועצה וקשר רצוף עם הנהלות מוסדות החינוך ועם רכזי ההסעות כדי לעדכן אותם בממצאי בדיקות האירועים החריגים ובטיפול המחייב הנדרש.

8. מובן שנושאים שלא בהכשרת הממונה, יוכלו להיבדק בידי גורם מקצועי או שהממונה ייווצץ בגורם כזה לשם השגת רמת בטיחות ראויה.
9. מומלץ, כי ממונה הבטיחות גם יבחן קיום ההוראות בדבר הסעות תלמידים בחינוך המיוחד והדרכת המלווים והנחייתם לגבי חובתם ואחריותם לשמירה ולדיווח.
10. כאמור, הביקורת ממליצה להגדיר תפקיד של מנהל מטה בטיחות כמובא בחוזר מנכ"ל משרד הפנים שיעסוק גם בבקרה בתחום השטח. באשר לכך ניתן למנות, בין היתר ומעבר לתפקידים המוגדרים של מנהל מטה הבטיחות, מספר תפקידים:

א. ביקורת על חברת ההסעות, רכבי ההסעה – בדיקה כללית ולא כתחליף לאחריות קצין הבטיחות, בקרות יזומות, בדיקה לאור תלונות;
ב. קשר לפתרון בעיות ולהתנהלות נכונה עם: חברות ההסעה, בתי הספר, מוקד המועצה, מחלקת התחבורה;
ג. ביקורת נהגים, התנהלות, נהיגה, התנהגות;
ד. עמידה בזמנים;
ה. העלאה והורדה בתחנות;
ו. הקפדה על כללי הבטיחות;
ז. התנהגות תלמידים;
ח. טיפול בבעיות אלימות;

ט. נוכחות והתנהלות המלווים;

י. תיקון ליקויים מבקרות קודמות של המועצה או של גורמים אחרים כמשכ"ל.

11. פיקוח, פיצויים ותיעוד – כמפורט להלן, על המועצה לראות בסעיפי הפיקוח והפיצויים בהסכם עם קבלני ההסעות ככלי ליעילות ולבטיחות ההסעות. מטרת התיעוד היא להוות כלי ואומדן להיקף וסוג ההפרות, ומטרת הפיצויים הינם להוות גורם הרתעה ומניעה להישנות ההפרות. מומלץ לתעד ולנתח את ההפרות, לבחון תיקון ליקויים ולהסיק מסקנות.
12. ליווי – אומנם ליווי בידי מבוגר הינו חובה רק בהסעת תלמידי החינוך המיוחד הזכאים לליווי בהתאם לחוק, אך ראוי להזכיר את שנכתב בחוזר המנכ"ל, כי רצוי שרכב המסיע ילדים ילווה על ידי אדם מבוגר - הורה, מורה וכדומה - ובמיוחד בהסעות אזוריות שבהן מסלול הנסיעה ארוך. הביקורת ממליצה לבחון אפשרויות שונות ובכלל זה – הליווי – בכדי לדאוג לבטיחות התלמידים לא רק במובן בטיחות הנסיעה, אלא גם מבחינת מוגנות מאלימות ופגיעות שונות.
13. העברת מידע - כלי נוסף להגברת הפיקוח והבקרה הוא המידע.
14. הביקורת ממליצה להעביר את הוראות הדין, הנחיות משרד החינוך והוראות הסכם ההתקשרות בתחום הבטיחות בין המועצה לחברות ההסעה לידיעת מנהלי מוסדות החינוך, על מנת שתשומת ליבם תופנה לענייני הבטיחות הנדרשים ובהתאם לכך יוכלו יותר לפקח, לדרוש ולעדכן את המועצה.
15. כמו כן, מומלץ להעביר מידע בהיר ונגיש להורים, למורים ולתלמידים על תחום הבטיחות בהסעות ועל הנדרש מהם, וכן דרכי התקשרות עם מוקד המועצה וגורמים נוספים הממונים על התחום.
16. לדעת הביקורת, על המועצה לדרוש מקציני הבטיחות של חברות ההסעה להגיש דיווחים תקופתיים על עמידתם של כלי הרכב המבצעים את ההסעות בדרישות הבטיחות, ולצרף לדיווחים את המסמכים הנקובים בחוזה ההסעות האחיד, זאת נוסף על הפיקוח שעל המועצה לבצע על ההסעות מתוקף תפקידה ולפי חוזר המנכ"ל.
17. לדעת הביקורת, מלבד דרישת דיווחים שוטפים, על המועצה לערוך ביקורות פתע ולדרוש נתונים ללא התראה מראש, ולא להסתמך על העובדה שלחברה יש קצין בטיחות מטעמה.
18. חשוב לזכור, שהגורם המרכזי לתאונות הדרכים הוא הגורם האנושי – הנהג. מלבד יתר המרכבים החשובים שבאחריות המועצה שפורטו בדוח הקודם, על המועצה לדאוג להדרכה מקצועית של כל הנהגים ולא להסתפק בדיווח על הדרכה של חברות ההסעה פעם בשנה. יש

לוודא אצל הנהגים את הבנתם ומחויבותם להנחיות ובין היתר להחתימם על טופס ההנחיות. ובכלל, חשוב "לתדלק" ולהוסיף לרצון, למודעות, ולמקצועיות בתחום הבטיחות.

19. ההוראות המסדירות את הסעת תלמידים ובכללן ההנחיות לגבי העלאת תלמידים והורדתם, נועדו למנוע את סיכון התלמידים. על המועצה לבקר, לפקח ולאכוף על קבלני ההסעות את קיום הוראות הבטיחות ובכללן הנוגעות להעלאה וההורדה של התלמידים בצמידות למדרכה ובמקומות המסומנים ובטיחותיים בלבד רק מהדלת הקדמית. בהקשר לכך חוזר המנכ"ל מזכיר, כי באוטובוס גובה המדרגות עולה על הגובה המקובל, ולאור זאת יש להקפיד על זהירות בעליה וביריד ממנו. כך גם מומלץ לוודא הדרכת התלמידים בבתי הספר בדבר ירידה ועליה לאוטובוס בזהירות ובמתינות וכאמור רק מהדלת הקדמית.
20. הביקורת ממליצה למועצה ולחברי הוועדה להוביל את הוועדה לבטיחות בדרכים לתפקוד יעיל. וועדה זו יכולה להשפיע על הבטיחות בתחנות ההסעה של התלמידים. הוועדה יכולה לסייע למועצה ליצור שיתופי פעולה בין הגופים והכוחות הממסדיים, הציבוריים והוולונטריים, ולהניע תכניות פעולה לצמצום תאונות הדרכים באזור המועצה. חברי הוועדה כנציגי הציבור יכולים ליצור קשר בלתי אמצעי עם התושבים, ליזום פעילויות לצמצום מספר תאונות הדרכים ולפעול להגברת מודעות הציבור לנושאי הבטיחות בדרכים.
21. מעבר לקביעת הסדרי תנועה כראוי עם הגורמים המוסמכים, על המועצה לוודא שהסדרי התנועה שנקבעו אכן נעשים באופן המקצועי והמיטבי ביותר על מנת להגביר את רמת הבטיחות.

פניות תושבים

ממצאי מבקר המדינה: "המועצה ניהלה רישום חלקי על תלונות בנוגע למהלך התקין של ההסעות המתקבלות במוקד המועצה. בשנות הלימודים התשע"ח - התש"פ נרשמו במוקד המועצה 256 תלונות בנוגע להסעות, רובן (172 תלונות, כ-67% מכלל התלונות) נסבו על איחור בהגעת רכב ההסעות (בד"כ 15 עד 30 דקות), לעיתים לגבי אותו קו הסעה. 26 מהתלונות נסבו על התנהלות לא נאותה של נהג ההסעה.

הבדיקה העלתה כי ברישום של רוב התלונות לא צוינו פרטי חברת ההסעות, מס' הטלפון של המתלונן ולעיתים אף לא יעד בית הספר שאליו הוסע התלמיד. כמו כן, לא נוהל מעקב אחרי הטיפול בתלונות ואחר תוצאות הטיפול.

עוד העלתה הבדיקה כי במהלך שנות הלימודים התשע"ח-התש"פ התקבלו במועצה 26 תלונות בכתב בנושא התנהלות לא הולמת של נהגי חברות ההסעות, בעקבותיהן התריעה

המועצה על דרישת פיצויים מוסכמים ואולם עלה כי המועצה דרשה פיצויים על חברות ההסעות רק בעקבות שמונה מהתרעותיה.

המועצה האזורית **לכיש** מסרה כי בעקבות הערת הביקורת, היא פתחה תיק לניהול ולרישום של תלונות או הערות מתושבי האזור״.

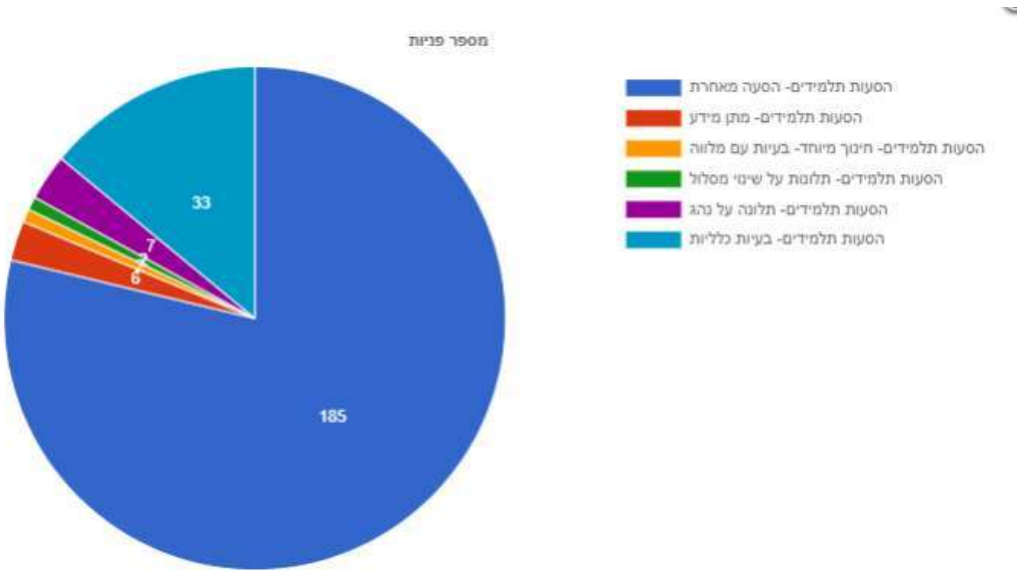
בבדיקת המצב בדוח לשנת 2021 נמסר ממחלקת תחבורה, כי במחלקה נפתח תיק פניות הכולל פניות ישירות למחלקה, אך הוא לא כולל את כלל תיעוד הפניות למוקד המועצה ולגורמים שונים מטעם המועצה.

בביקורת הנוכחית לבדיקת תיקון הליקוי, נמצא כי עדיין אין תיעוד ממוחשב מסודר כולל של כל פרטי הפונים, מהות הפניות, מועדי הפניות, מצב הטיפול בפניות וכיו״ב.

כל הפניות למחלקה מתועדות בתיקיה ידנית.

כמו כן, עדיין מרבית הפניות למוקד המועצה עוסקות באיחורים.

להלן נתוני פניות לשנים 2021-2022



<u>דוגמאות של פניות למוקד – ינו׳-נוב׳ 22</u>

על מנת להתרשם מהפניות למוקד, הביקורת ליקטה חלק מהפניות (בעיבוד עמ״נ להשמיט פרטי פונים).

ההסעה מאחרת ביותר מחמש דקות
ההסעה מאחרת בדקות רבות
איחור ההסעות

בוקר טוב. הבוקר איחרה ההסעה לשער הנגב פעם שלישית החודש. הילדים עומדים בקור למעלה מ20 דקות.
הסעה מאשל הנשיא מאחרת בכמה דקות זאת הפעם העשרים
הילדים חיכו כבר יום שני להסעה שעתיים בגשם ובקור
הסעה חזור ללכיש מאשל הנשיא מאחרת זו הפעם ה22
הסעה מאחרת ללכיש מאשל הנשיא זו הפעם ה30
ההסעה לרבקה גובר
הסעה איחרה היום (11.2.2022) בעשרים דקות!!!!
הסעה לא הגיעה לקחת את הבן שלה מכרמי גת בחזרה לאחוזם. הילד מחכה שם
אוטובוס לצפית
הסעה שהייתה צריכה להגיע לאסוף מאשל הנשיא ב 13:35 עדיין לא הגיעה. איחור כבר של עשר דקות ועדיין לא הגיעה
במושב לכיש ההסעות של הילדים מתעקבות בחזרה פניוה חוזרת
במושוב לכיש ההסעות של הילדים מאחרת בחזרה
בכל יום א' ההסעה של אליאב מאחרת בצורה מוגזמת ! היום איחרה בשעה עגולה!!!
ההסעה מקבוצת יבנה לאליאב היתה צריכה להגיע ב 1315 ומאחרת. הסדרן אמר שתגיע רק ב 14
הסעת תלמידי לובה אליאב שהיתה אמורה לצאת לפני כ45 דקות לשדה משה עדיין לא אספה את התלמידים הצעירים
איחור הסעה
ההסעה מקבוצת יבנה לאליאב מאחרת בקביעות בימי חמישי
הסעות יסודי ותיכון טרם הגיעו

הסעה של השעה 14:45 מאחרת כבר 20 דק הילדים מחכים ועדיין לא הגיעה לידיעה וטיפול בבקשה.
הסעה מאחרת מלובה אליאב איחור של יותר מחצי שעה
הסעות ללובה אליאב מאחרות. דבר שחוזר על עצמו. צריך שיהיה אופציה למעקב אחר מיקום ההסעה. והמינימום שיהיה עדכון על איחור לנציגים במושב.
הסעת איסוף תלמידי בהס "ריבקה גובר" בימי שישי מגיע ועוזב את תחנות ההסעה מוקדם מהזמן הנקוב | בתאריך 06.05 האוטובוס כבר יצא מהישוב בשעה 07:27 כאשר הוא אמור להיות בתחנה הראשונה ב 07:30 - נאלצנו להתארגן ולהסיע את הילדים (שלנו ועוד ילדים שעמדו בתחנה) בכוחות עצמינו לבה"ס
לא היה מקום בהסעה של לובה אליאב לשדה משה והילדים המתינו לאוטובוס נוסף
לא היה מקום בהסעה חזור וכמה ילדים כולל הבת שלי היו צריכים להמתין שנסעה נוספת תגיע
הסעה מאחרת להגיע ולפזר את הילדים בשעה שלמה !!! לא מתקבל על הדעת.
איחור של כמעט שעה
ההסעות של הקייטנה שוב מאחרות וההסעה מלאה ולילדים אין איפה לשבת
הסעה של הקייטנה מאחרת הגיעה ב8:20 לשדה משה
אתמול יום ראשון ההסעה הגיעה ב8.20 במקום ב7.40 היום יום שני לקייטנה ההסעה הגיעה ב8.12 במקום ב7.40 מדובר בילדים קטנים שרוצים להגיע לקייטנה בזמן בשעה 8.00 וגם אין מקום בהסעה אנו מבקשים שתעשו סדר החל ממחר
יום שלישי ברציפות הסעה מאחרת הגיעה למושב ב8:05

ההסעה שוב מאחרת לקייטנה של לובה אליאב
ההסעה לקייטנת לובה אליאב שוב מאחרת בחצי שעה
הסעה מאחרת שדה משה לקייטנה לובה אליאב הגיעה רק ב8 ועשרה למושב
איחור הסעה כבר בוקר 3 ברציפות לקייטנה בלובה אליאב
הסעת ילדים שוב מאחרת בכחצי שעה. נשמח אם יפצלו את ההסעות כמו תמיד. האיחורים פוגעים גם הפרנסה של ההורים
איחור זמנים הגעה להסעות הילדים
כל בוקר בזמן הקייטנה ההסעה מגיעה באיחור של חצי שעה. הילדים מאחרים למסגרת וגם משתוללים ליד הכבישים ומסכנים עצמם. ש
האם יש הסעות לבית ספר עוברת ממועצה חוף אשקלון לניר חנבית ספר שקמה ביד מרדכי
פניה חוזרת ביקשה לדעת אם יש הסעות בניר חן לבית ספר שיקמה
הסעה לאשל הנשיא אחרה ב40 דקות
לגבי הסעות צהרון בית ספר יצחק גובר רוצה לדבר עם המחלקה
הסעת ילדים ללובה אליאב מאחרת. עכשיו 08:10 והיא עדין לא הגיעה
איחור הסעה
הסעה לא הגיעה משדה משה ללובה אליאב הייתה צריכה להגיעה ב7:40
הסעה שניה לבית הספר לובה אליאב הגיעה ב8:45!!!!
איחור של הסעה בשעה היום בבוקר ללובה אליאב
איחורים בלתי נסבלים בהסעות. עבר היום כל גבול!
איחור תמידי בהסעות - הסעה שאמורה לצאת לבית ספר אשל הנשיא בשעה 6:50 יוצאת ממנוחה רק בשעה 7:30. זה בלתי אפשרי להתעסק בזה כל בוקר!!! מבקשת התייחסותכם. תודה.

הסעה אשל הנשיא מאחרת. פעם שניה מתוך ארבע הסעות שהיו עד עכשיו
הסעה של לובה אליאב מאחרת
הסעה קבוצת יבנה אליאב מאחרת (אחור שני ב3 ימים)
הסעה מקבוצת יבנה היתה אמורה להגיע ב15.25 עדיין לא הגיעה גם ב1/9 איחרה
ההסעה מיבנה עוד לא הגיעה ליבנה כבר חצי שעה אחרי סיום הלימודים
אוטובוס מקבוצת יבנה איחר ב-50 דקות
איחור הסעה לובה אליאב הגיעה ב8:00
איחור הסעה
הסעה של לובה אליאב הגיעה ב8 למושב
ההסעת תלמידים מאחרת כבר יומיים-בבוקר-כנראה כי נוסע קודם למנוחה תחנות 1 2 3
שוב איחור של האוטובוס חזרה מבית ספר קבוצת יבנה חוסר אחריות של החברה וגם המועצה שלא מטפל בזה
הסעות מאחרות בהמון זמן בדרכ יותר משעה בכל משך. השבוע מאליאב לבני דקלים והפוך. גם ביסודי וגם באולפנה. לא הגיוני!
מאז תחילת השנה כבר שבוע שההסעה מאליאב לביהס נועם בבני דקלים יוצאת באיחור גדול מאוד. הילדים ממתינים לה מ-7:45 ועד ל-8:30. הם מאחרים בקביעות לשיעור הראשון. זו אמורה להיות הסעה שאוספת לפני כן את כרמי קטיף אבל בפועל היא מגיעה לאליאב הרבה פעמים כשהיא ריקה. עובדה שמעידה על כך שהנהג כבר הוריד את ילדי כרמי קטיף בביה"ס ומשאיר את ילדי אליאב להמתין לו משך זמן רב בשעה שכבר אין כמעט מבוגרים ביישוב (למעט פועלי בניין שישנם בשפע...)

ההסעה מאחרת בחזרה מהלימודים. הגיע אוטובוס אחד בלבד. ושאר הילדים מחכים בחום בבית הספר עד שההסעה שלהם תגיע. ממה שנראה אותו אוטובוס מביא את שני הסבבים. אנחנו הורי .. לא מוכנים למסכת העינויים שהילדים שלנו עוברים. מבקשת טיפול משמעתי חמור מול חברת ההסעות.
הסעה של לובה אליאב שעה 12:45 מאחרת- ככל הנראה הסעה אחת יצאה עם כיתות א ב והיתר נשארו בבית ספר שאותו אוטובוס יחזור לאסוף אותם
איחור בהסעה הילדים סיימו ב 13:00 ועדיין מחכים בבית הספר לאוטובוס הביתה.
ההסעה איחרה
הילדים מחכים מהשעה 13:00!!!
הסעה מאחרת
ילד בן 7 מחכה לאוטובוס שייקח אותו הביתה כבר קרוב לחמישים דקות
הסעת תיכונים מאחרת מכרמי גת לשדה. משה
ההסעה חזרה מבית ספר איחרה בשעה
איחור ללובה אליאב
8:08 וההסעה לבני דקלים עדיין לא הגיעה
ההסעה לא הגיעה עדיין 8.10
הסעה מאחרת
ההסעה שוב איחרה ב20 דק האוטובוס הסריח מסיגריות והילד שלי עם אסתמה נזקק למשאף בשל כך
| חמישה ל8 הגיעה ההסעה | וכל האוטובוס עם ריח חזק של סיגריות.
אתמול הגיע אוטובוס אחד בלבד לאיסוף בשעה 13:00 ונותרו תלמידים רבים ללא הסעה והמתינו כמעט שעה לאוטובוס נוסף כאשר ברור

שמראש לא נשלחו שתי הסעות. היום בבוקר שוב איחרה ההסעה הפעם רק" ברבע שעה אך האוטובוס היה עם ריח חריף של סיגריות. לא ברור לי למה ילדים צעירים צריכים להכנס לאוטובוס אפוף עשן וריח סיגריות."
חזור הסעה מאחרת ב 40 דקות ויותר מכרמי גת לשדה משה
אין הסעות!!! הילדים מחכים יותר מחצי שעה או שעה כדי שנסעה תבוא לקחת אותם בבוקר או בצהריים
בתאריך 8.9 הסעות החזור מבית הספר לובה אליאב התעכבו יותר משעה!! מדובר בילדים קטנים משכבות א-ד שנאלצו לחכות יותר משעה כדי לחזור הביתה. מבירור עם ביהס הסעות הגיעו ולא היה מספיק מקום לכולם ולכן נאלצו לפזר את כולם ורק אז לחזור כדי לקחת את שאר הילדים. לא מקובל בכלל. חשוב לציין שזו ממש לא הפעם הראשונה אנחנו סובלים מעניין זה כבר כמה שנים. גם בבוקר וגם בסוף היום. אי אפשר להמשיך ככה!"
הילדים בכרמי גת מחכים כל יום שעה שלמה להסעה בחזור הביתה. ככה אי אפשר להמשיך. חייבים למצוא פתרון ומהר
הבעיות עם ההסעות לבני דקלים ממשיכות: כל השבוע ההסעה הגיעה באיחור גדול (כחצי שעה-3/4 שעה איחור). היום ההסעה הגיעה ואספה רק מתחנה אחת. לתחנה העליונה ברחוב החרוב היא כלל לא הגיעה. רק בשעה 9:00 אחד ההורים עבר באיזור מצא את הילדים ממתינים והסיע אותם בעצמו.
הסעה מאחרת מתחילת שנה תיכון כרמי גת לשדה משה
איחור הסעה לובה אליאב בחזרה
ההסעה הגיעה רק עכשיו 8:05
הסעה מאחרת

אשל הנשיא. היא מגיעה באיחור באופן קבוע והתלמידים מאחרים קבוע
ההסעה לאשל הנשיא איחרה בהרבה
הסעה חזרה מבית ספר על יסודי קבוצת יבנה מסריח כמו שתן ממש מגעיל ולא מקובל כל בילדים סובלים נורא
אוטובוס חזרה מבית ספר יסודי מלובה אליאב איחר לאיסוף ב-40 דקות לא בסדר—ילדים מחכים בחוץ
עקיפה מסכנת חיים של רכב הסעות הסעה שיצאה מלובה אליאב ב13 הנהג עקף טור מכוניות ארוך על קו הפרדה רצוף תוך סיכון חייהם של הנוסעים לטיפולכם הדחוף !
הסעה חזרה של בה״ס העל יסודי קבוצת יבנה משריך כמו עישון ומאוד קשה לילדים לשבת שם
הסעה חזרה מבי״ס שוב איחר
ההסעה איחרה היום ב 20 ד
הסעה מאחרת
ההסעה של בי"ס מאחרת משמעותית באופן כמעט קבוע
הסעה לאשל הנשיא מאחרת
הסעה לאשל הנשיא הגיעה באיחור של חצי שעה
שוב אוטובוס חזרה בה״ס על יסודי קבוצת יבנה באיחור
הסעה הגיעה ב8
הסעה לאשל הנשיא מאחרת
הסעה לאשל הנשיא מגיעה רק בשעה 7:40 כששעה ראשונה מתחילה ב 08:00!!!!
הסעות
איחור באיסוף בבוקר אשל הנשיא

הנהג הגיע באיחור ונזכר בבית קמה ששכח לאסוף את ילדי אחוזם וחזר בחזרה ולכן הילדים איחרו לשיעור!!!!!
הסעה אשל הנשיא
הסעה מאחרת כרגיל !!!!
הסעות אשל הנשיא
הסעות שוב מאחרים בחלוקה
דיווח על נהג בהסעה משער הנגב לנהורה ביום ראשון 2.10 בשעה 15:30
ההסעה מאחרת בלמעלה מחצי שעה. כל השבוע המצב דומה. אך היום חמור במיוחד.
הסעה מאחרת קבועעעע
בתאריך 25.10 ההסעה של בית ספר האלה בנחושה שיוצאת ממעלה רחוב החרוב הגיעה באיחור. במקום להגיע ב-7:25 הגיעה רק ב-7:50.
תלונה ל23.10- הסעה מאחרת מעל 20 דקות מאליאב לביהס האלה נחושה
תלונה ל24.10 הסעה מאחרת מעל 20 דקות מאליאב לביהס האלה נחושה אירוע לחוזר על עצמו
תלונה מתאריך 25.10 איחור בהסעה של מעל 20 דקות מאליאב לביהס האלה נחושה
איחור בהסעות
הסעה יצאה ללא הילדים מבית הספר הנהג אמר שלא עוצר בשדה משה. לאחר שהיו מספר רב של פניות לאחראי הסעות ישראל ההסעה חזרה ואספה אותם. הנהג נסע בפראות לא בזהירות לא האט בבאמפרים ולא רצה לעצור בתחנות בטענה שממהר לעשות הסעה

אחרת. פשוט הזוי ולא הגיוני בעליל שככה מתעללים בילדים שלנו. שמתי את הדיווח תחת קטגוריה של תלונה על הנהג אבל לא פחות מזה התלונה שלי מופנית למועצה שלא מסדירה את נושא ההסעות משדה משה לאשל הנשיא ובכל פעם מחדש עולות תלונות אחרות.
הסעה חזרה מביס האלה (נחושה) מלוכלכת ומסריחה מסיגריות"
השעה 14:55 ואין הסעה לילדים שסיימו בשעה 13:00 !!!
הסעות תלמידים -אשל הנשיא
הבן שלי לומד באשל הנשיא. היום סיים ללמוד בשעה 14:00 ורק ב 14:40 ההסעה הגיעה. עכשיו השעה 15:20 והוכ עדיין לא בבית!!!!!!!! פשוט בושה שזו ההתנהלות יום אחרי יום!
בהמשך לתלונה הקודמת שפתחתי היום בנוגע לאיחור בהסעות ההסעה של הילדים יצאה בסופו של דבר מבית ספר אשל הנשיא רק בשעה 15:00. שעתיים לאחר סיום הלימודים
הסעה לנחושה הגיעה באיחור של חצי שעה עם נהג שלא ידע לאן הוא נוסע
ההסעה אחרה היום ביותר מחצי שעה!!! זה לא סביר ולא נסבל!!! אני רק מקווה שהנהג לא ינהג בפראות כדי להשלים את הזמן האבוד
ההסעה משפרינצק לאליאב מאחרת הם עדין לא הגיעו הביתה. הבנו מהילדים שהיא חזרה לקרית גת אחרי שהגיעה לצומת לכיש. לא מגיע לילדנו יחס שכזה
במקום 2 אוטובוסים הגיעו אוטובוס ומיניבוס והיו ילדים שישבו על הרצפה לא חגורים!
לא הביאו אוטובוס לילדים והם ישבו על רצפת המיניבוס והאוטובוס!!וסכנת נפשות

ההסעה לבית ספר האלה בנחושה יצאה הבוקר באיחור של חצי שעה עם נהג חדש שלא מכיר את התחנות בישוב ולא את הדרך. הילדים הגיעו לבית ספר ביום שישי כמעט בתשע! היו יכולים כבר להשאר בבית
בנסעה חזור מבית ספר האלה הגיעו אוטובוס ומיניבוס במקום 2 אוטובוסים. לא היה מקום לכל הילדים ויחדים ישבו על הרצפה!!
הסעות שבאו לאסוף מנחושה שבוע שעבר בלי מספיק מקומות ישיבה לתלמידים
הסעה לנחושה איחרה
ההסעה מאליאב לנחושה הבוקר איחרה בחצי שעה!
הסעה אליאב לביהס האלה התעכבה הבוקר בחצי שעה
קו 61 לעוצם בוטל ביקש לדעם אם אפשר להחזיר האוטובוס
ההסעה שחזרה מבית ספר האלה לאליאב היתה מטונפת. הרצפה והמושבים היו כל כך מלוכלכים שילדים רבים נותרו עומדים. לצערנו תופעה זו חוזרת שוב ושוב בהסעות חזור.
איחורים חוזרים ונשנים ילדים מאחרים לחוגים יש לכך עלות כספית שאנו ההורים והילדים משלמים. נוסף לזה עייפות של ילדים ושחיקה של הילדים ושלנו. די! טפלו בנושא ההסעות. זה ממש ביזיון
אומנם כותב פה פעם ראשונה אבל כל יום יש מה לכתוב... היום ההסעה פשוט לא הגיעה ולא היה מקום אז ההסעה החלופית הגיעה באיחור של 40 דקות. נמאס שאתם מזלזלים בחינוך ובחיים של הילדים שלנו. כשיקרה אסון זה על הראש שלכם (דני וישראל)
הסעה מאחרת
ההסעה איחרה ובמקום שני אוטובוסים הגיע אוטובוס ומיניבוס
חברת ההסעות רמת נגב לנסיעה מאליאב לבית ספר האלה שוב שלח מי יבוס במקום אוטובוס. אין מספיק מקום לכל הילדים.

הסעה לובה אליאב
נהג הסעות תלמידים בנסיעה ללכיש נסע במהירות מופרזת של מעל 120 קמש תוך סיכון ילדינו. לא מקובל בשום רמה בטיחות ילדינו מעל הכל.

מנהל מחלקת התחבורה מסר כי עקב הפניות ורצון המועצה לתקן, עד לינואר 2023 יוקם מוקד פניות ייעודי שיפעל מ 06:30 בבוקר ועד 19:00 בערב ויתופעל בידי משכ"ל כפיילוט. המנהל מסר שעושה מאמץ גדול על מנת למנוע כל תקלה עליה מלינים ההורים בפניות לעיל ובכלל ובנוסף למוקד הייעודי, המועצה נרתמת לשיפור מתמיד של מערך ההסעות בכל ההיבטים.

<u>המלצות</u>

הביקורת חוזרת על המלצתה מדוח 2021 כלשונה למועצה ולמחלקת התחבורה לראות בפניות משאב ולא מטרד. מדובר בכל הפניות: פניות טלפוניות, דוא"ל, פניות למוקד וכו'.

כעולה מפניות ההורים, קיימת בעיית שירות בתחום ההסעות (טענות כלפי נהגים מסוימים), ועל המועצה לבדוק את הפניות ולטפל בנושא זה בהקדם.

לפניות חשיבות רבה שכן מלבד הצורך בטיפול נקודתי בכל פניה, הפניות מהוות את אחד הכלים לפיקוח ובקרה על איכות ההסעה.

על כל הגורמים המטפלים בתחום ההסעות להתייחס במהירות וביעילות לפניות הורים, המלווים ונציגי מוסדות החינוך.

מלבד הצורך בטיפול בפניות הקונקרטיות, יש לעשות שימוש בכלל הפניות ככלי ומנוף לשם ייעול וטיוב מערך הסעות התלמידים.

לדעת הביקורת וכאמור לעיל, קיים צורך בקביעת נוהל טיפול בפניות. כך למשל, יש לתעד את פרטי הפונים, מהות הפניות, מועדי הפניות, מצב הטיפול בפניות וכיו"ב. הביקורת ממליצה על תיעוד ממוחשב שיכלול את כלל הפרטים ויוכל לשמש ככלי עבודה יעיל.

מומלץ לתעד את הפניות והטיפול בהן באופן כזה שניתן יהיה להפיק לקחים, לתקן ליקויים ולשפר את התנהלות מערך הסעות התלמידים.

תחנות ההסעה

בבית ספר בבני דקלים – בשנת 2021 נוספה גדר בטיחות ונצפתה יותר הקפדה על אי חניית הורים בתחנת ההסעה. בביקורת חוזרת בשטח בשנה זו – 2022 נצפתה אחראית שמונעת ירידה לא בטיחותית של ילדים לכביש, אך עדיין נצפו הורים עוצרים וחונים את מכוניותיהם בתחנות ההסעה באופן מסוכן.

הביקורת מצאה שוב תקלות בטיחות. הורים המעבירים את ילדיהם – וכן ילדים שעוברים לבדם – שלא דרך המדרכות ואף מעבר למעקות הבטיחות ובין אוטובוסים בעת עצירתם להורדת תלמידים בבית ספר בנהורה.

כדי להציב את הדברים כדיוקם, הביקורת חוזרת על ממצאי עובדי משרד מבקר המדינה אשר בדקו את תחום תחנות ההסעה בשלושה בתי ספר בתחומי שיפוטה של המועצה וכן בתחנות הסעה בחמישה יישובים והעלו את הממצאים הבאים בלשון זו:

1. בתחנות האיסוף וההורדה בבית הספר ביישוב בני דקלים - שבו לומדים כ-800 תלמידים, 100 תלמידי גנים וכן עובדים כ-80 עובדי הוראה - אכן הותקנו גדרות הפרדה, ואולם התחנות אינן מקורות, אינן מסוככות ואינן בנויות במתחם פנימי. כפי שניתן לראות בתמונה 4, קשה להמתין בהן בעת שהשמש קופחת או בעת שיורד גשם. עוד עלה כי במקומות המסומנים כמיועדים לתחבורה ציבורית חונות מכוניות פרטיות של מורים והורים. נוסף על כך, לא נשמרים כללי הבטיחות הן בעת שמאות תלמידים המגיעים לבית הספר בו בזמן בארבעה-חמישה אוטובוסים, והן בעת שעשרות מכוניות מתוך היישוב מורידות בבית הספר תלמידים (שאינם זכאים להסעות). גם בסוף יום הלימודים, בעת שמתבצע איסוף של חלק גדול מהתלמידים באותה שעה, שורר דוחק רב במקום והבטיחות אינה נשמרת, כפי שניתן לראות היטב בסרטון המצורף שצולם ביום גשום.[49]

כך למשל, הובא בדוח כי בתחנות הסעה בכניסה לבית הספר הממ"ד בני דקלים, תחנות ההסעה אינן מקורות, והן אף אינן מרוכזות במתחם נפרד אלא פזורות בכניסה לבית הספר.

המועצה האזורית **לכיש** מסרה בתשובתה ממרץ 2021 למבקר המדינה כי **בני דקלים** הוא יישוב חדש, תחנת האיסוף הקיימת בו היא זמנית בלבד (אך עומדת בקריטריונים שפורטו בחוזר המנכ"ל מדצמבר 2018), וכבר התקבל ממשרד התחבורה אישור לתכנון תחנה קבועה לאיסוף ולהורדה של תלמידים, ואולם כיוון שהתכנון תוקצב בחסר המועצה נמצאת בשלב של "איגום תקציבי" והיא מקווה להתקדם בבנייתה עוד השנה.

2. בכביש פנימי, בסמוך לכניסה וליציאה לבתי הספר ע"ש "לובה אליאב" ביישוב **לכיש** וע"ש רבקה גובר ביישוב **נהורה**, פזורות תחנות הסעה מקורות, המוגנות באמצעות גדרות הפרדה, כנדרש מהבחינה הבטיחותית.

49 ראו כתובת ביוטיוב https://www.youtube.com/watch?v=JEGcj3pF7Bc.

3. עוד עלה כי בכל היישובים שנבדקו נמצא כי תחנות ההסעה מקורות, ואולם, לא הותקנו ביניהן ובין הכביש הראשי העובר ביישוב גדרות הפרדה כנדרש.

בעניין זה מסרה המועצה האזורית בתשובתה כי אין היא סבורה שנקבעה הנחיה או תקנה ולפיה יש להתקין מעקות בטיחות החוצצים בין חזית התחנה לכביש.

עוד נמסר לביקורת ממחלקת ההנדסה, כי תחנת האיסוף בבני דקלים אומנם זמנית, אך עונה על הקריטריונים הנדרשים. תחנת האיסוף הקבועה קיבלה אישור ממשרד התחבורה והיא בשלב איגום תקציבי (היא תוקצבה בחסר בידי משרד התחבורה), בתקווה להתקדם לביצועה עוד בשנת למודים זו (התשפ"ב). כמו כן, ישנה כוונה להשלים 5 תחנות מקורות בתחנות איסוף בני דקלים במגבלות התקציב.

בביקורת תיקון הליקויים במסגרת ביקור בשטח במספר פעמים, התברר כי המועצה עדיין לא תיקנה את הליקוי:

תמונה מנוב' 2022:

יבורך בית הספר בבני דקלים והשיטור הקהילתי שמבצע עם התלמידים משמרות בטיחות וזהירות בדרכים. משיחות הביקורת עם מורים ותלמידים עולה כי הדבר מוסיף לבטיחות ולמודעות.

מנהל מחלקת התחבורה מסר כי כיום באיסוף בבוקר, נמצא פתרון להקטנת העומס על ידי עצירת האוטובוסים במפרץ נוסף לפני תחנת ההסעה הנוכחית. פתרון זה לא עונה על הליקוי של תחנות ההסעה ועל העומס בפיזור.

ממחלקת הנדסה נמסר, כי תוך ימים ספורים (בתחילת דצמ׳ 2022) יחלו בביצוע מגרש חניה גדול לרכבים פרטיים עם כניסה נפרדת שלא צמודה לחניית האוטובוסים. מגרש חניה זה יקל על העומס בסמוך לבית הספר וכן יצמצם בעיות בטיחות.

הביקורת מברכת על הפתרונות ועל הכוונה לכניסה לביצוע מהיר, ואולם גם פתרון זה לא עונה על הליקוי בתחנות ההסעה כאמור לעיל.

המלצות

מבקר המדינה קבע, כי על המועצה האזורית לכיש להסדיר את שמירת כללי הבטיחות בסביבות תחנות האיסוף וההורדה בבתי ספר ביישוב בני דקלים ובכביש הגישה אליהם. כדי להגביר את בטיחות התלמידים המחכים לרכבי ההסעות בתחנות האיסוף והפיזור של תלמידים בכל יישובי המועצה, מוטלת עליה החובה להתקין מעקות הפרדה.

הביקורת חוזרת על המלצותיה מדוח הביקורת לשנת 2021 בעניין תחנות ההסעה ושוב מעירה על הצורך למלא אחר כל דרישות הבטיחות כולל גידור, הפרדה, סימוני מעברי חציה, אמצעי האטת כלי רכב ושילוט כנדרש. הקפדה על הקמת תחנות הסעה תקניות ועל מילוי דרישות הבטיחות תסייע לצמצום פגיעות ותאונות ומחויבת לשם שמירת שלומם וחייהם של התלמידים המוסעים.

לדעת הביקורת, שמירת הבטיחות מחייבת פעולות, גם כאלו שלא מפורשות בתקנות ובהנחיות.

הביקורת קוראת לפעול באופן מיידי לתיקון ולהעלאת רמת הבטיחות במסופי ההסעה הסמוכים לבתי הספר בהתאם להמלצותיה ולנדרש בהתאם לנסיבות.

בדוח הביקורת לשנת 2021 הביקורת קראה למועצה לפעול באופן מיידי וראשוני באמצעות קיום ההוראות המחייבות של הדין וחוזר מנכ"ל.

כמו כן, הומלץ לקדם תוכניות חינוכיות ולפעול מול ההורים בנוגע לאחריותם כלפי ילדיהם בתחנות האיסוף וההורדה, בזמן הנסיעה, בחציית כביש ובכל הכרוך בנסיעה למוסדות החינוך ובחינוך ילדיהם לשמירת הבטיחות.

זאת ועוד, הומלץ על הדרכה והקפדה מול הנהגים גם בכל הכרוך לסביבת תחנות ההסעה. כך למשל, יש להדריך את הנהגים שלא יחלו בנסיעה עד להשלמת עלייתם או ירידתם של התלמידים מרכב ההסעה והתרחקות ממנו עד למרחק ללא סכנה מפני פגיעה מרכב זה או מרכבים אחרים. יש למנוע מצבים שבהם התלמידים לא יהיו בשדה הראיה של הנהגים.

לדעת הביקורת, ראוי לשלב עד כמה שניתן פעילות משטרתית באזור הסעות התלמידים (ולפעול עם משמרות בטיחות בדרכים בשילוב התלמידים בעוד בתי ספר ברחבי המועצה). מלבד התחום הביטחוני, שלא נדון בדוח, מדובר גם בהיבט בטיחותי. פעילות שיטור גלויה וסמויה תביא לשיפור נהיגה והקפדה על שמירת חוקי התנועה של נהגים, הורים והולכי הרגל.

הסעת תלמידים ללא שימוש בחגורות בטיחות ובעמידה

בבדיקת תיקון הליקויים בתחום חגירת החגורות, הביקורת חוזרת על ממצאיה והמלצותיה. נמצא שהליקוי לא תוקן.

בדיקה חוזרת, כולל פניית הורים, העלתה כי עדיין רבים מהתלמידים אינם חגורים. נצפו מספר מקרים של תלמידים שהוסעו בעמידה.

הסעת תלמידים ללא חגורות ובעמידה חושפת אותם לסכנה. על המועצה לפעול לאכיפת תקנות התעבורה והוראות הסכמי ההסעות בכל הקשור לחגורות הבטיחות ולנסיעה בעמידה ולנקוט אמצעים נגד הקבלנים המפרים את הוראות הבטיחות.

פסולת נהורה

1. מתוך כוונה טובה לטובת התושבים ולצורך מיחזור, החל מאמצע שנת 2021 הוקמה פינת מיחזור גדולה – עם מתקני מיחזור לסוגי הפסולת השונים - בסמוך למבנה משרדי המועצה.
2. בדוח 2021 עלה כי פינה זו על מתקניה, אינה מסודרת, פסולת רבה מושלכת סביב למתקני המחזור, פסולת רגילה הושלכה לפחים לא מתאימים, אריזות הושלכו על בסמוך לפחים, חלק מהפסולת מתעופפת ברוח.
3. מנהל המחלקה החליט לנעול תחנת מחזור זו. בבירור חוזר של הביקורת בשנת 2021 התקבלה תשובה, שהמועצה בהליכי התקשרות עם חברה לצורך שדרוג כל תחנות המחזור במועצה.
4. לאורך שנת 2022 המצב נשאר כפי שהיה וניתן לראות זאת בתמונות המצורפות.
5. הביקורת ערכה ביקורת חוזרת ו"ביקור במקום" מספר פעמים בסמוך למכולות נהורה ושדה דוד ואף ביקור במכולת מנוחה. המצב נראה הרבה יותר טוב. יש זמנים שיש בהם יותר עומס. קיימת הקפדה בעיקר בנושא הקרטונים. נדרש שדרוג לטיפול בשאר סוגי הפסולת.

דוח ביקורת משרד הפנים

1. **דוח מבקר משרד הפנים – 2020 - הועבר לעיון הביקורת בסוף יוני 2022.**

2. **ועדת הביקורת דנה בדוח משרד הפנים. בישיבה הודגש, כי בפרק ב' לדוח נכתב: "לא נמצאו ליקויים בשנת הדוח" והוועדה בירכה על כך.**

3. **הועדה בדקה את תיקון הליקויים בתחום ועדות הביקורת. בדוח מבקר משרד הפנים נמצא כי תוקן ליקוי מהעבר בדבר אי מינוי כל ועדות הביקורת. כאמור בדוח הנוכחי, הוועדות לא מתפקדות והביקורת מעירה כי אין די לדון רק בליקוי בנושא מינוי ועדות (שגם על כך לא קיבלו נתונים מדויקים), אלא גם בתפקודם.**

4. **המועצה קיימה דיון בדוח משרד הפנים לשנת 2020 ובהמלצות ועדת הביקורת ביום 28/06/22.**

5. **מבקר משרד הפנים הפנה לנספח 2 לטופס 1 בדוחות הכספיים (עמ' 27), אשר נכללו בהם, לפי נתוני אגף הגביה, חובות מסופקים בסך 35,146 אלפי ₪, המהווים כ 57% מהסך הכולל של החייבים ליום 31 בדצמבר 2020. (ליום 31 בדצמבר 2019 35,433 אלפי ₪, המהווים כ- 59% מהסך הכולל של החייבים) וכן לביאור 16 (בעמ' 22) לדוחות הכספיים שעניינו התחייבויות תלויות ובו מדווח על 5 תביעות כנגד המועצה תלויות ועומדות, נכון ליום 31 לדצמבר 2020 שאינן בתחום הכיסוי הביטוחי – בהתבסס על כך ובהתאם לחוו"ד של היועץ המשפטי, נכללה בדוחות הכספיים הפרשה על סך של 1,437 אלפי ₪ בתקציב הרגיל.**

תודה רבה למבקר המועצה.

אני רואה בביקורת כלי עבודה ועזר לעבודה יעילה וחסכונית, וזאת מלבד תפקידה לבחון ולבדוק את פעולות המועצה האם היא פועלת לפי הדין וסדרי מינהל תקינים.

<u>תחום אבטחת המידע והפרטיות –</u>

השתכנעתי בדבר הצורך לשפר את מצבנו ולהעלות את רמת אבטחת המידע וככלל ההמלצות מקובלות.

ברור לכולנו שמערכות המיחשוב ומאגרי המידע משמשים את המועצה בפעילותה המגוונת ושבמאגרי המידע יש נתונים חשובים ובהם גם נתונים אישיים על התושבים.

הסכנה בפגיעה במערכות המיחשוב ובמאגרי המידע היא גם לפרטיות וגם לעבודה השוטפת של המועצה.

מבקר המועצה צודק בהחלט שעלינו להגן על מערכות המיחשוב והמידע ולאחר לימוד הדוח, מובן יותר שעל המועצה להגביר את האבטחה לשם שמירת הפרטיות, אבטחת המידע, שיפור השירות ועבודת המועצה לטובת התושבים.

לאור הממצאים וההמלצות בדוח זה, אני מבקש ממנכ"ל המועצה ללמוד את הדוח ולגבש צוות בליווי מקצועי, שיביא להעלאת הרמה בתחום אבטחת המידע והפרטיות במועצה.

בהתאם לעולה מהדוח ולפי הנדרש לפי הדין ולפי הצורך, הצוות יגבש המלצות מעשיות עם סדרי עדיפויות. נראה שראשית יש להביא ליישום ההמלצות המחויבות לפי הדין.

קיימות גם המלצות בדוח שעוסקות בשיפור שאינו נדרש לפי החוק ומטיל עומס תקציבי על המועצה כגון מינוי ממונה הגנת הפרטיות.

ייתכן וכמו שהמבקר ציין, ישנן המלצות שניתן ליישם בתקציב נמוך, ועם זאת, אין זה נכון בעיניי ליישם המלצות שאיננו חייבים בהן לפני שנקבל עצה והמלצה מאנשי מקצוע.

<u>ועדות ביקורת</u>

בממצאים המובאים בדוח, מובא שהמועצה תזכרה את הוועדים בחובתם בעניין ועדות הביקורת.

המועצה לא אמורה להחליף את הוועדים בתפקיד חשוב זה.

במשך הזמן המועצה גם תזכרה את הוועדים וגם מינתה חברים לועדות הביקורת.

הדוח מעלה את אי התפקוד של ועדות הביקורת, ואכן יש לפעול בנושא.

אני מקבל את ההמלצה להדריך את הוועדים. ביצענו זאת בעבר ונציע זאת גם בהמשך.

<u>ההסעות</u>

כמו שהסברתי בעבר ובתגובה לדוח קודם, בשנים האחרונות גדלנו וכך גם מספר התלמידים ומספר מוסדות הלימוד שבהם לומדים תלמידנו היקרים.

אנחנו בתהליך שיפור מתמיד. הדברים עולים גם בדוח.

העלינו את רמת הדרישות ממשכ"ל ומחברות ההסעה, תיקי הנהגים מסודרים, מתקיימות בקרות, נפתח תיק פניות ומענה משמעותי לפניות תושבים, שמים דגש על העלאת רמת הבטיחות, מחלקת תחבורה עובדת עם מערכת ממוחשבת לניהול ההסעות, משקיעים מאמצים רבים ועלויות לשם שיפור לוחות הזמנים בהגעה אל בתי הספר ובחזרה לבתים ועוד.

אנו פועלים מעל ומעבר בתכנון ובעשייה השוטפת לאורך כל השנה.

אני מקבל את תגובת מנהל מחלקת התחבורה לגבי השיפור בתחום הבטיחות, מיצוי התקציב ממשרד החינוך ושיפור המענה לפניות התושבים.

מכיר היטב ומקבל את תגובת מנהל מחלקת התחבורה והגזבר, שהמועצה מוציאה על תחום ההסעות יותר ממה שמקבלת ממשרד החינוך.

לשם שיפור תחום הבטיחות, כמו שביקשתי בעבר, מבקש ממנכ"ל המועצה לכנס פורום שיכלול את הגורמים הנדרשים ובכללם מנהל מחלקת התחבורה, מהנדס המועצה, מנהלת מחלקת חינוך וקב"ט

המועצה. אבקש מפורום זה שיפיק מסקנות מדוח זה ומהמציאות בשטח, יביא המלצות ליישום ויעדכן אף את המליאה.

בעניין העיכובים וההמתנות, תמיד יש מקום לשפר ואנו עושים מאמצים ניכרים לכך, אך איננו יכולים לספק הסעה אישית ומונית לכל תלמיד ותלמידה. נוסיף ונתאמץ בנושא ככל יכולתנו.

אני בקשר שוטף עם ההורים וכמובן עם מנהלי מחלקות חינוך והסעות, מקבל תושבים לפגישות בנושא ומציג בפניהם את התמונה הכוללת. כמו שמסר מנהל מחלקת התחבורה, בקרוב יופעל כפיילוט מוקד ייעודי לתחום ההסעות. אנו מעוניינים לשמוע את הציבור ולהשתפר ככל יכולתנו.

נספח א'

חוק הגנת הפרטיות, תשמ"א-198150

פרק א': פגיעה בפרטיות

איסור הפגיעה בפרטיות

1.

לא יפגע אדם בפרטיות של זולתו ללא הסכמתו.

פגיעה בפרטיות מהי

2.

פגיעה בפרטיות היא אחת מאלה:

(1)

בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;

(2)

האזנה האסורה על פי חוק;

(3)

צילום אדם כשהוא ברשות היחיד;

(4)

פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;

4(א)

50 מאתר נבו.

פרסום תצלומו של נפגע ברבים שצולם בזמן הפגיעה או סמוך לאחריה באופן שניתן לזהותו ובנסיבות שבהן עלול הפרסום להביאו במבוכה, למעט פרסום תצלום בלא השהיות בין רגע הצילום לרגע השידור בפועל שאינו חורג מהסביר באותן נסיבות; לעניין זה" ,נפגע – "מי שסבל מפגיעה גופנית או נפשית עקב אירוע פתאומי ושפגיעתו ניכרת לעין;

(5)

העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו; לענין זה" ,כתב – "לרבות מסר אלקטרוני כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;

(6)

שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם ריווח;

(7)

הפרה של חובת סודיות שנקבעה בדין לגבי עניניו הפרטיים של אדם;

(8)

הפרה של חובת סודיות לגבי עניניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;

(9)

שימוש בידיעה על עניניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;

(10)

פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או;(9)

(11)

פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, לרבות עברו המיני, או למצב בריאותו, או להתנהגותו ברשות היחיד.

פרסום תצלום של נפטר

2א. (א)

לעניין חוק זה רואים כפגיעה בפרטיות גם פרסום ברבים של תצלום גופת אדם גלויה באופן שניתן לזהותה, אלא אם כן התקיים אחד מאלה:

(1)

אותו אדם הסכים בחייו לפגיעה כאמור;

(2)

חלפו 15 שנים ממועד פטירתו של אותו אדם;

(3)

התקבלה הסכמה לפגיעה כאמור מאת הראשון מבין המפורטים בפסקאות משנה (א) עד (ד), שעודו בחיים, ובלבד שהנפטר לא התנגד בחייו לפגיעה כאמור וילדו או הורהו לא הודיע למפרסם או לאחר מטעמו כי הוא מתנגד לפרסום:

(א)

בן זוגו;

(ב)

כל ילדיו;

(ג)

הוריו;

(ד)

כל אחיו;

(4)

לא היו לנפטר קרובי משפחה המנויים בפסקה (3) ובית המשפט אישר את הפרסום.

(ב)

בן זוגו של נפטר, ילדו, הורהו או אחיו רשאים להגיש תובענה אזרחית בשל פרסום לפי סעיף זה.

הגדרת מונחים

3.

לענין חוק זה–

"אדם – "לענין סעיפים 2, 7, 13, 14, 17ב, 17ג, 17ו, 17ז, 23א, 23ב ו-25 – למעט תאגיד;

"הסכמה – "הסכמה מדעת, במפורש או מכללא;

"מחזיק, לענין מאגר מידע" – מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש;

"פרסום – "כמשמעותו בסעיף 2 לחוק איסור לשון הרע, התשכ"ה-1965;

"צילום – "לרבות הסרטה.

"שימוש – "לרבות גילוי, העברה ומסירה.

פגיעה בפרטיות – עוולה אזרחית

.4

פגיעה בפרטיות היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש], יחולו עליה בכפוף להוראות חוק זה.

פגיעה בפרטיות – עבירה

.5

הפוגע במזיד בפרטיות זולתו, באחת הדרכים האמורות בסעיף 2(1), (3) עד (7) ו-(9) עד (11), דינו – מאסר 5 שנים.

מעשה של מה בכך

.6

לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש.

פרק ב': הגנה על הפרטיות במאגרי מידע

הגדרות

.7

בפרק זה ובפרק ד–'

"אבטחת מידע – "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;

"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;

"מידע – "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;

"מידע רגיש– "

(1)

נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2)

מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

"מנהל מאגר – "מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;

"רשם – "מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, והממשלה מינתה אותו, בהודעה ברשומות, לנהל את פנקס מאגרי מידע (להלן – הפנקס) כאמור בסעיף 12 ;

"שימוש", במידע – (נמחקה);

"שלמות מידע – "זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

סימן א': מאגרי מידע

רישום מאגר מידע והשימוש בו

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.

(ב)

לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

(ג)

בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

(1)

מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;

(2)

יש במאגר מידע רגיש;

(3)

המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;

(4)

המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;

(5)

המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.

(ד)

הוראת סעיף קטן (ג) לא תחול על מאגר שאין בו אלא מידע שפורסם לרבים על פי סמכות כדין או שהועמד לעיון הרבים על-פי סמכות כדין.

(ה)

הרשם רשאי, מטעמים מיוחדים שיירשמו, להורות על קיום חובת רישום לגבי מאגר הפטור מחובת רישום לפי סעיפים קטנים (ג) ו-(ד); הוראה כאמור תומצא לבעל המאגר ובה יפרט הרשם הוראות לענין ניהול ואחזקת המאגר עד לרישומו.

בקשה לרישום

9(א)

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.

(ג)

שר המשפטים רשאי לקבוע בתקנות פרטים נוספים שיפורטו בבקשה לרישום.

(ד)

הבעל או המחזיק של מאגר מידע יודיע לרשם על כל שינוי בפרט מהפרטים המפורטים בסעיף קטן (ב) או לפי סעיף קטן (ג) ועל הפסקת פעולתו של מאגר המידע.

סמכויות הרשם

10(א)

הוגשה בקשה לרישום מאגר מידע–

(1)

ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין;

(2)

הרשם רשאי לרשום מטרה שונה מזו שפורטה בבקשה, לרשום מספר מטרות למאגר, או להורות על הגשת מספר בקשות תחת הבקשה שהוגשה, והכל אם נוכח לדעת כי הדבר הולם את פעילות המאגר הלכה למעשה;

(3)

הרשם לא יסרב לרשום את מאגר המידע לפי פסקה (1) ולא יפעיל סמכויותיו לפי פסקה (2), אלא לאחר שנתן למבקש הזדמנות לטעון את טענותיו.

(ב) (בוטל)

(ב1)

לא רשם הרשם את מאגר המידע תוך 90 ימים מיום שהוגשה לו הבקשה, ולא הודיע למבקש על סירובו לרשום או על השהיית הרישום מטעמים מיוחדים שיפרט בהודעתו – רשאי יהיה המבקש לנהל או להחזיק את המאגר אף שאינו רשום.

(ב2)

הודיע הרשם למבקש על סירובו לרשום את מאגר המידע, או על השהיית הרישום כאמור בסעיף קטן (ב1) לא יהיה המבקש רשאי לנהל או להחזיק את המאגר, זולת אם בית המשפט קבע אחרת.

(ב3)

הרשם ימחק רישומו של מאגר מידע מהפנקס, אם הודיע לו בעל המאגר שהמידע שבאותו מאגר בוער, ואימת הודעה זו בתצהיר; הוחזק מאגר מידע שלא בידי בעל מאגר המידע, תאומת ההודעה גם בתצהיר של המחזיק.

(ג)

הרשם יפקח על מילוי הוראות חוק זה והתקנות לפיו.

(ד)

שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקים בצו, יחידת פיקוח שתפקח על מאגרי המידע, רישומם ואבטחת המידע בהם; גודלה של היחידה יותאם לצורכי הפיקוח.

(ה)

הרשם יעמוד בראש יחידת הפיקוח, והוא ימנה את המפקחים לצורך ביצוע הפיקוח לפי חוק זה; לא יתמנה למפקח אלא מי שקיבל הכשרה מקצועית מתאימה בתחום מיחשוב ואבטחת מידע והפעלת סמכויות לפי חוק זה, ומשטרת ישראל לא הביעה התנגדות למינויו מטעמים של שמירה על בטחון הציבור.

(ה1)

לצורך ביצוע תפקידיו רשאי מפקח–

(1)

לדרוש מכל אדם הנוגע בדבר למסור לו ידיעות ומסמכים המתייחסים למאגר מידע;

(2)

להיכנס למקום שיש לו יסוד סביר להניח כי מופעל בו מאגר מידע, לערוך בו חיפוש ולתפוס חפץ, אם שוכנע כי הדבר דרוש לשם הבטחת ביצוע חוק זה וכדי למנוע עבירה על הוראותיו; על חפץ שנתפס לפי סעיף זה יחולו הוראות פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969; סדרי כניסה למיתקן צבאי או למיתקן של רשות בטחון כמשמעותה בסעיף 19(ג) ייקבעו על ידי שר המשפטים בהתייעצות עם השר הממונה על רשות הבטחון, לפי הענין; בפסקה זו" ,חפץ – "לרבות חומר מחשב, ופלט כהגדרתם בחוק המחשבים, התשנ"ה-1995;

(3)

על אף הוראות פסקה (2), לא ייכנס למקום כאמור המשמש למגורים בלבד, אלא לפי צו מאת שופט של בית משפט שלום.

(ו)

הפר מחזיק או בעל של מאגר מידע הוראות של חוק זה או התקנות לפיו, או לא מילא אחר דרישה שהפנה אליו הרשם, רשאי הרשם להתלות את תוקפו של הרישום לתקופה שיקבע או לבטל את רישומו של מאגר המידע בפנקס, ובלבד שקודם להתליה או לביטול ניתנה לבעל המאגר הזדמנות להשמיע את טענותיו.

(ז)

דין הרשם ומי שפועל מטעמו כדין עובד המדינה.

דוח הגנה על הפרטיות

10א .

לא יאוחר מ-1 באפריל בכל שנה תגיש המועצה להגנת הפרטיות לועדת החוקה חוק ומשפט של הכנסת דין וחשבון שיכין הרשם על פעולות האכיפה והפיקוח בשנה שקדמה להגשת הדוח, בצירוף הערותיה של המועצה.

חובת מבקש מידע

.11

פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה–

(1)

אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו;

(2)

המטרה אשר לשמה מבוקש המידע;

(3)

למי יימסר המידע ומטרות המסירה.

פנקס מאגרי מידע

12(א)

הרשם ינהל פנקס מאגרי מידע אשר יהיה פתוח לעיונו של הציבור.

(ב)

הפנקס יכיל את הפרטים לרישום מאגר המידע כאמור בסעיף 9 .

(ג)

על אף הוראות סעיפים קטנים (א) ו-(ב), במאגר של רשות בטחון, הפרטים המפורטים בסעיף 9(ב)(3), (4) ו-(5) לא יהיו פתוחים לעיונו של הציבור.

זכות עיון במידע

13(א)

כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

(ב)

בעל מאגר מידע יאפשר עיון במידע, לפי בקשת אדם כאמור בסעיף קטן (א) (להלן – המבקש), בשפה העברית, הערבית או האנגלית.

(ג)

בעל המאגר רשאי שלא למסור למבקש מידע המתייחס למצבו הרפואי או הנפשי אם לדעתו עלול המידע לגרום נזק חמור לבריאותו הגופנית או הנפשית של המבקש או לסכן את חייו; במקרה זה ימסור בעל המאגר את המידע לרופא או לפסיכולוג מטעמו של המבקש.

(ג1)

אין בהוראות סעיף זה כדי לחייב למסור מידע בניגוד לחסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחסיון נועד לטובתו.

בסעיף קטן זה" ,דין – "לרבות הלכה פסוקה.

(ד)

האופן, התנאים והתשלום למימושה של זכות העיון במידע ייקבעו בתקנות.

(ה)

הוראות סעיף זה וסעיף 13א לא יחולו–

(1)

על מאגר מידע של רשות בטחון כמשמעותה בסעיף 19(ג);

(1א)

על מאגר מידע של שירות בתי הסוהר;

(2)

על מאגר מידע של רשות מס כמשמעותה בחוק לתיקון דיני מסים (חילופי ידיעות בין רשויות מס), התשכ"ז-1967;

(3)

כשבטחון המדינה, יחסי חוץ שלה או הוראות חיקוק מחייבים שלא לגלות לאדם מידע שעליו.

(4)

על מאגר מידע של גופים אשר שר המשפטים בהתייעצות עם שר הבטחון או עם שר החוץ, לפי הענין, ובאישור ועדת החוץ והבטחון של הכנסת, קבע כי הוא כולל מידע שבטחון המדינה או יחסי החוץ שלה מחייבים שלא לגלותו (להלן – מידע סודי), ובלבד שאדם המבקש לעיין במידע שעליו המוחזק באותו מאגר יהיה זכאי לעיין במידע שאינו מידע סודי.

(5)

על מאגר מידע אודות חקירות ואכיפת החוק של רשות המוסמכת לחקור על פי דין בעבירה, אשר שר המשפטים קבע אותה בצו, באישור ועדת החוקה חוק ומשפט של הכנסת.

(6)

על מאגר מידע שהוקם לפי סעיף 28 לחוק איסור הלבנת הון, התש"ס-2000.

עיון במידע שאינו בהחזקת בעל המאגר

13א .

בלי לגרוע מהוראות סעיף 13–

(1)

בעל מאגר מידע, המחזיק אותו אצל אחר (בסעיף זה – המחזיק), יפנה את המבקש אל המחזיק, תוך ציון מענו, ויורה למחזיק, בכתב, לאפשר למבקש את העיון;

(2)

פנה המבקש תחילה למחזיק, יודיע לו המחזיק אם הוא מחזיק מידע עליו, וכן את שם בעל מאגר המידע ואת מענו.

תיקון מידע

14(א)

אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ – למחזיק מאגר המידע, בבקשה לתקן את המידע או למוחקו.

(ב)

הסכים בעל מאגר המידע לבקשה כאמור בסעיף קטן (א), יבצע את השינויים הנדרשים במידע שברשותו ויודיע עליהם לכל מי שקיבל ממנו את המידע בתקופה שנקבעה בתקנות.

(ג)

סירב בעל מאגר המידע למלא בקשה כאמור בסעיף קטן (א), יודיע על כך למבקש, באופן ובדרך שנקבעו בתקנות.

(ד)

מחזיק חייב לתקן מידע, אם בעל מאגר המידע הסכים לתיקון המבוקש או שבית משפט ציווה על התיקון.

תובענה לבית המשפט

15.

על סירובו של בעל מאגר מידע לאפשר עיון כאמור בסעיף 13 או בסעיף 13א ועל הודעת סירוב כאמור בסעיף 14(ג), רשאי מבקש המידע להגיש תובענה לבית המשפט באופן ובדרך שנקבעו בתקנות.

סודיות

16.

לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי; אם הוגשה הבקשה לפני תחילת ההליך תידון הבקשה בבית משפט השלום. המפר הוראות סעיף זה, דינו – מאסר 5 שנים.

אחריות לאבטחת מידע

17.

בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

מחזיק במאגרים של בעלים שונים

17א. (א)

מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

(ב)

מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי

המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

ממונה על אבטחה

17ב. (א)

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

(1)

מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(2)

גוף ציבורי כהגדרתו בסעיף 23;

(3)

בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

(ב)

בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

(ג)

לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

סימן ב': דיוור ישיר

הגדרות

17ג .

בסימן זה–

"דיוור ישיר – "פניה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי איפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע;

"פניה – "לרבות בכתב, בדפוס, בטלפון, בפקסימליה, בדרך ממוחשבת או באמצעי אחר;

"שירותי דיוור ישיר – "מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא.

דיוור ישיר

17ד .

לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן הוא רשום בפנקס ואחת ממטרותיו הרשומות היא שירותי דיוור.

ציון מקור המידע

17ה .

לא ינהל אדם ולא יחזיק מאגר מידע המשמש לשירותי דיוור ישיר, אלא אם כן יש בידו רישום המציין את המקור שממנו קיבל כל אוסף נתונים המשמש לצורך מאגר המידע ומועד קבלתו, וכן למי מסר כל אוסף נתונים כאמור.

מחיקת מידע ממאגר המשמש לדיוור ישיר

17ו. (א)

כל פניה בדיוור ישיר תכיל באופן ברור ובולט–

(1)

ציון כי הפניה היא בדיוור ישיר, בצירוף ציון מספר הרישום של המאגר המשמש לשירותי דיוור ישיר בפנקס מאגרי מידע;

(2)

הודעה על זכותו של מקבל הפניה להימחק מן המאגר כאמור בסעיף קטן (ב); בצירוף המען שאליו יש לפנות לצורך כך;

(3)

זהותו ומענו של בעל מאגר המידע שבו מצוי המידע שעל פיו בוצעה הפניה, והמקורות שמהם קיבל בעל המאגר מידע זה.

(ב)

כל אדם זכאי לדרוש, בכתב, מבעל מאגר מידע המשמש לדיוור ישיר, שמידע המתייחס אליו יימחק ממאגר המידע.

(ג)

כל אדם זכאי לדרוש, בכתב, מבעל מאגר המידע המשמש לשירותי דיוור ישיר או מבעל מאגר המידע שבו מצוי המידע שעל-פיו בוצעה הפניה, כי מידע המתייחס אליו לא יימסר לאדם, לסוג בני אדם או לאנשים מסויימים, והכל לפרק זמן מוגבל או קבוע.

(ד)

הודיע אדם לבעל מאגר המידע על דרישתו כאמור בסעיפים קטנים (ב) או (ג), יפעל בעל המאגר בהתאם לדרישה ויודיע לאדם, בכתב, כי פעל על פיה.

(ה)

לא הודיע בעל מאגר המידע כאמור בסעיף קטן (ד) תוך 30 ימים מיום קבלת הדרישה, רשאי האדם שהמידע מתייחס אליו לפנות לבית משפט השלום בדרך שנקבעה בתקנות, כדי שיורה לבעל מאגר המידע לפעול כאמור.

(ו)

הזכויות לפי סעיף זה של נפטר שרשום במאגר מידע נתונות גם לבן זוגו, לילדו, להורהו או לאחיו.

תחולה על ידיעות

17ז .

הוראות סימן זה יחולו על ידיעות הנוגעות לענייניו הפרטיים של אדם, אף שאינם בגדר מידע, כשם שהן חלות על מידע.

אי תחולה על גוף ציבורי

17ח .

סימן זה לא יחול על גוף ציבורי כמשמעותו בסעיף 23(1) במילוי תפקידיו על פי דין.

שמירת דינים

17ט .

הוראות סימן זה באות להוסיף על הוראות כל דין.

פרק ג': הגנות

הגנות מה הן

18.

במשפט פלילי או אזרחי בשל פגיעה בפרטיות תהא זו הגנה טובה אם נתקיימה אחת מאלה:

(1)

הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי סעיף 13 לחוק איסור לשון הרע, התשכ"ה-1965;

(2)

הנתבע או הנאשם עשה את הפגיעה בתום לב באחת הנסיבות האלה:

(א)

הוא לא ידע ולא היה עליו לדעת על אפשרות הפגיעה בפרטיות;

(ב)

הפגיעה נעשתה בנסיבות שבהן היתה מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה;

(ג)

הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע;

(ד)

הפגיעה נעשתה תוך ביצוע עיסוקו של הפוגע כדין ובמהלך עבודתו הרגיל, ובלבד שלא נעשתה דרך פרסום ברבים;

(ה)

הפגיעה היתה בדרך של צילום, או בדרך של פרסום תצלום, שנעשה ברשות הרבים ודמות הנפגע מופיעה בו באקראי;

(ו)

הפגיעה נעשתה בדרך של פרסום שהוא מוגן לפי פסקאות (4) עד (11) לסעיף 15 לחוק איסור לשון הרע, התשכ"ה-1965;

(3)

בפגיעה היה ענין ציבורי המצדיק אותה בנסיבות הענין, ובלבד שאם היתה הפגיעה בדרך של פרסום – הפרסום לא היה כוזב.

פטור

19(א)

לא ישא אדם באחריות לפי חוק זה על מעשה שהוסמך לעשותו על פי דין.

(ב)

רשות בטחון, או מי שנמנה עם עובדיה או פועל מטעמה, לא ישאו באחריות לפי חוק זה על פגיעה שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו.

(ג)

"רשות בטחון ,"לענין סעיף זה – כל אחד מאלה:

(1)

משטרת ישראל;

(2)

אגף המודיעין במטה הכללי והמשטרה הצבאית של צבא-הגנה לישראל;

(3)

שירות בטחון כללי.

(4)

המוסד למודיעין ולתפקידים מיוחדים.

(5)

הרשות להגנה על עדים.

נטל ההוכחה

20(א)

הוכיח הנאשם או הנתבע שעשה את הפגיעה בפרטיות באחת הנסיבות האמורות בסעיף 18(2) ושהפגיעה לא חרגה מתחום הסביר באותן נסיבות, חזקה עליו שעשה את הפגיעה בתום לב.

(ב)

חזקה על הנאשם או הנתבע שעשה את הפגיעה בפרטיות שלא בתום לב אם הוא פגע ביודעין במידה גדולה משהיתה נחוצה באופן סביר לצורך הענינים שניתנה להם הגנה בסעיף 18.(2)

(ג)

חזקה על נאשם או נתבע הטוען להגנה על פי סעיף 18(2)(ב) או (ד) שעשה את הפגיעה בפרטיות שלא בתום לב, אם ביצע את הפגיעה תוך כדי הפרת הכללים או העקרונות של אתיקה מקצועית החלים עליו מכוח דין או המקובלים על אנשי המקצוע שהוא נמנה עמהם; ואולם חזקה כאמור לא תחול אם הפגיעה נעשתה בנסיבות שבהן הנאשם או הנתבע פעל בהתאם לחובה חוקית המוטלת עליו.

הפרכה של טענות הגנה

21.

הביא הנאשם או הנתבע ראיה או העיד בעצמו כדי להוכיח אחת ההגנות הניתנות בחוק זה, רשאי התובע להביא ראיות סותרות; אין בהוראה זו כדי לגרוע מסמכות בית המשפט לפי כל דין להתיר הבאת ראיות בידי בעלי הדין.

הקלות

22.

בבואו לגזור את הדין או לפסוק פיצויים רשאי בית המשפט להתחשב, לטובת הנאשם או הנתבע, גם באלה:

(1)

הפגיעה בפרטיות לא היתה אלא חזרה על מה שכבר נאמר, והוא נקב את המקור שעליו הסתמך;

(2)

הוא לא התכוון לפגוע;

(3)

אם היתה הפגיעה בדרך של פרסום – הוא התנצל על הפרסום ונקט צעדים להפסקת מכירתו או הפצתו של עותק הפרסום המכיל את הפגיעה, ובלבד שההתנצלות פורסמה במקום, במידה ובדרך שבהם פורסמה הפגיעה ולא היתה מסוייגת.

פרק ד': מסירת מידע או ידיעות מאת גופים ציבוריים

הגדרות

23.

בפרק זה–

"גוף ציבורי– "

(1)

משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין;

(2)

גוף ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, ובלבד שבצו ייקבעו סוגי המידע והידיעות שהגוף יהיה רשאי למסור ולקבל;

(3)(נמחקה)

"מאגר מידע", "מידע", "הרשם" ו"שימוש" – (נמחקו).

תחולה על ידיעות

23א .

הוראות פרק זה יחולו על ידיעות על עניניו הפרטיים של אדם, אף שאינן בגדר מידע, כשם שהן חלות על מידע.

איסור על מסירת מידע

23ב. (א)

מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה.

(ב)

אין בהוראות סעיף זה כדי למנוע מרשות בטחון כמשמעותה בסעיף 19 לקבל או למסור מידע לשם מילוי תפקידה, ובלבד שהמסירה או הקבלה לא נאסרה בחיקוק.

סייג לאיסור

23ג .

מסירת המידע מותרת, על אף האמור בסעיף 23ב, אם לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית–

(1)

בין גופים ציבוריים, אם נתקיים אחד מאלה:

(א)

מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע והיא דרושה למטרת ביצוע חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

(ב)

מסירת המידע היא לגוף ציבורי הרשאי לדרוש אותו מידע על פי דין מכל מקור אחר;

(2)

מגוף ציבורי למשרד ממשלתי או למוסד מדינה אחר, או בין משרדים או מוסדות כאמור, אם מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

אולם לא יימסר מידע כאמור שניתן בתנאי שלא יימסר לאחר.

חובותיו של גוף ציבורי

23ד. (א)

גוף ציבורי המוסר דרך קבע מידע בהתאם לסעיף 23ג יפרט עובדה זו על כל דרישת מידע בהתאם לחוק.

(ב)

גוף ציבורי המוסר מידע בהתאם לסעיף 23ג יקיים רישום של המידע שנמסר.

(ג)

גוף ציבורי המקבל דרך קבע מידע בהתאם לסעיף 23ג, והמידע נאגר במאגר מידע, יודיע על כך לרשם ועובדה זו תיכלל בפרטי רשימת מאגרי המידע לפי סעיף 12.

(ד)

גוף ציבורי שקיבל מידע בהתאם לסעיף 23ג לא יעשה בו שימוש אלא במסגרת הסמכויות או התפקידים שלו.

(ה)

לענין חובת השמירה על סודיות לפי כל דין, מידע שנמסר לגוף ציבורי מכוח חוק זה, כמוהו כמידע שאותו גוף השיג מכל מקור אחר, ובנוסף יחולו על הגוף המקבל גם כל ההוראות החלות על הגוף המוסר.

מידע עודף

23ה. (א)

מקום שמידע שמותר למסרו לפי סעיפים 23ב או 23ג מצוי על גבי אותו קובץ עם מידע אחר (להלן – מידע עודף), רשאי הגוף המוסר את המידע למסור לגוף המקבל את המידע המבוקש עם המידע העודף.

(ב)

מסירת מידע עודף לפי סעיף קטן (א) מותנית בקביעת נוהלים שיבטיחו מניעת שימוש כלשהו במידע עודף שנתקבל; נוהלים כאמור ייקבעו בתקנות וכל עוד לא נקבעו בתקנות, יקבע הגוף המבקש נוהלים כאמור בכתב, וימציא לגוף המוסר עותק מהם, לפי דרישתו.

מסירה מותרת אינה פגיעה בפרטיות

23ו .

מסירת מידע המותרת לפי חוק זה לא תהווה פגיעה בפרטיות ולא יחולו עליה הוראות סעיפים 2 ו-8.

תקנות לענין מסירת מידע

23ז .

שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, רשאי להתקין תקנות בדבר סדרי מסירת מידע מאת גופים ציבוריים.

עונשין

23ח. (בוטל)

פרק ה': שונות

דין המדינה

24.

חוק זה חל על המדינה.

מות הנפגע

25(א)

אדם שנפגע בפרטיותו ותוך ששה חדשים לאחר הפגיעה מת בלי שהגיש תובענה או קובלנה בשל אותה פגיעה, רשאים בן-זוגו, ילדו או הורהו, ואם לא השאיר בן-זוג, ילדים או הורים – אחיו או אחותו, להגיש, תוך ששה חדשים לאחר מותו, תובענה או קובלנה בשל אותה פגיעה.

(ב)

אדם שהגיש תובענה או קובלנה בשל פגיעה בפרטיות ומת לפני סיום ההליך, רשאים בן-זוגו, ילדו או הורהו, ואם לא השאיר בן-זוג, ילדים או הורים – אחיו או אחותו, להודיע לבית המשפט, תוך ששה חדשים לאחר מותו, על רצונם להמשיך בתובענה או בקובלנה, ומשהודיע כאמור יבואו הם במקום התובע או הקובל.

התיישנות

.26

תקופת ההתיישנות של תביעה אזרחית לפי חוק זה היא שנתיים.

החלת הוראות מחוק איסור לשון הרע

.27

על הליכים משפטיים בשל פגיעה בפרטיות יחולו הוראות סעיפים 21, 23 ו-24 לחוק איסור לשון הרע, התשכ"ה-1965, בשינויים המחוייבים לפי הענין.

ראיות על שם רע, אופי או עבר של אדם

.28

במשפט פלילי או אזרחי בשל פגיעה בפרטיות אין להביא ראיה או לחקור עד בדבר שמו הרע של הנפגע או בדבר אפיו, עברו, מעשיו או דעותיו.

צווים נוספים

29(א)

בנוסף לכל עונש וסעד אחר רשאי בית המשפט, במשפט פלילי או אזרחי בשל הפרה של הוראה מהוראות חוק זה, לצוות כמפורט להלן, לפי הענין:

(1)

על איסור הפצה של עתקי החומר הפוגע או על החרמתו; צו החרמה לפי פסקה זו כוחו יפה כלפי כל אדם שברשותו נמצא חומר כזה לשם מכירה, הפצה או החסנה, גם אם אותו אדם לא היה צד למשפט; ציווה בית המשפט על החרמה, יורה מה ייעשה בעתקים שהוחרמו;

(2)

על פרסום פסק הדין, כולו או מקצתו; הפרסום ייעשה על חשבון הנאשם או הנתבע, במקום, במידה ובדרך שקבע בית המשפט;

(3)

על מסירת החומר הפוגע לנפגע.

(4)

על השמדת מידע שנתקבל שלא כדין, או לאסור על שימוש במידע כאמור או במידע עודף כהגדרתו בסעיף 23ה, או להורות לגבי המידע כל הוראה אחרת.

(ב)

אין בהוראות סעיף זה כדי למנוע החזקת עותק של פרסום בספריות ציבוריות, בארכיונים וכיוצא באלה, זולת אם הטיל בית המשפט, בצו החרמה על פי סעיף קטן (א)(1), הגבלה גם על החזקה כזאת, ואין בהן כדי למנוע החזקת עותק של פרסום בידי הפרט.

פיצוי בלא הוכחת נזק

29א. (א)

הורשע אדם בעבירה לפי סעיף 5, רשאי בית המשפט לחייבו לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק; חיוב בפיצוי לפי סעיף קטן זה הוא כפסק דין של אותו בית משפט שניתן בתובענה אזרחית של הזכאי נגד החייב בו.

(ב) (1)

במשפט בשל עוולה אזרחית לפי סעיף 4, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על 50,000 שקלים חדשים, בלא הוכחת נזק;

(2)

במשפט כאמור בפסקה (1) שבו הוכח כי הפגיעה בפרטיות נעשתה בכוונה לפגוע, רשאי בית המשפט לחייב את הנתבע לשלם לנפגע פיצוי שלא יעלה על כפל הסכום כאמור באותה פסקה, בלא הוכחת נזק.

(ג)

לא יקבל אדם פיצוי בלא הוכחת נזק לפי סעיף זה, בשל אותה פגיעה בפרטיות, יותר מפעם אחת.

(ד)

הסכומים האמורים בסעיף זה יעודכנו ב-16 בכל חודש, בהתאם לשיעור השינוי במדד החדש לעומת המדד הבסיסי; לענין זה–

"מדד – "מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;

"המדד החדש – "מדד החודש שקדם לחודש העדכון;

"המדד הבסיסי – "מדד חודש מאי 2007.

אחריות בשל פרסום בעתון

30(א)

פורסמה פגיעה בפרטיות בעתון, ישאו באחריות פלילית ואזרחית בשל הפגיעה האדם שהביא את הדבר לעתון וגרם בכך לפרסומו, עורך העתון ומי שהחליט בפועל על פרסום אותה פגיעה בעתון, ובאחריות אזרחית ישא גם המוציא לאור של העתון.

(ב)

באישום פלילי לפי סעיף זה תהא זאת הגנה טובה לעורך העתון שנקט אמצעים סבירים כדי למנוע פרסום אותה פגיעה ושלא ידע על פרסומה.

(ג)

בסעיף זה" ,עורך עתון – "לרבות עורך בפועל.

אחריות של מדפיס ומפיץ

.31

פורסמה פגיעה בפרטיות בדפוס, למעט בעתון בעל תדירות הופעה של ארבעים ימים או פחות, ישאו באחריות פלילית ואזרחית בשל הפגיעה גם מחזיק בית הדפוס שבו הודפס הפרסום, ומי שמוכר את הפרסום או מפיץ אותו בדרך אחרת, ובלבד שלא ישאו באחריות אלא אם ידעו או חייבים היו לדעת שהפרסום מכיל פגיעה בפרטיות.

עונשין בעבירות של אחריות קפידה

31א. (א)

העושה אחד מאלה, דינו – מאסר שנה:

(1)

מנהל, מחזיק או משתמש במאגר מידע בניגוד להוראות סעיף 8;

(2)

מוסר פרטים לא נכונים בבקשה לרישום מאגר מידע כנדרש בסעיף 9;

(3)

אינו מוסר פרטים או מוסר פרטים לא נכונים בהודעה המלווה בקשה לקבלת מידע לפי סעיף 11;

(4)

אינו מקיים את הוראות סעיפים 13 ו-13א לענין זכות העיון במידע המוחזק במאגר מידע, או אינו מתקן מידע על פי הוראות סעיף 14;

(5)

מאפשר גישה למאגר מידע בניגוד להוראות סעיף 17א(א) או אינו מוסר לרשם מסמכים או תצהיר בהתאם להוראות סעיף 17א(ב);

(6)

אינו ממנה ממונה על אבטחת מידע בהתאם להוראות סעיף 17ב;

(7)

מנהל או מחזיק מאגר המשמש לשירותי דיוור ישיר, בניגוד להוראות סעיפים 17ד עד 17ו;

(8)

מוסר מידע בניגוד לסעיפים 23ב עד 23ה.

(ב)

עבירה לפי סעיף זה אינה טעונה הוכחת מחשבה פלילית או רשלנות.

עוולה בנזיקין

31ב .

מעשה או מחדל בניגוד להוראות פרקים ב' או ד' או בניגוד לתקנות שהותקנו לפי חוק זה יהווה עוולה לפי פקודת הנזיקין [נוסח חדש].

חומר פסול לראיה

32.

חומר שהושג תוך פגיעה בפרטיות יהיה פסול לשמש ראיה בבית משפט, ללא הסכמת הנפגע, זולת אם בית המשפט התיר מטעמים שיירשמו להשתמש בחומר, או אם היו לפוגע, שהיה צד להליך, הגנה או פטור לפי חוק זה.

תיקון פקודת הנזיקין

.33

בפקודת הנזיקין [נוסח חדש], סעיף 34א – בטל.

תיקון חוק סדר הדין הפלילי

.34

בתוספת לחוק סדר הדין הפלילי, התשכ"ה-1965, אחרי פסקה (12) יבוא:

(13)"עבירות על חוק הגנת הפרטיות, התשמ"א-1981."

שמירת דינים

.35

הוראות חוק זה לא יגרעו מהוראות כל דין אחר.

ביצוע ותקנות

.36

שר המשפטים ממונה על ביצוע חוק זה והוא רשאי להתקין תקנות, באישור ועדת החוקה חוק ומשפט של הכנסת, בכל ענין הנוגע לביצועו, ובין השאר–

(1)

תנאי החזקת מידע ושמירתו במאגרי מידע;

(2)

תנאים להעברה של מידע אל מאגרי מידע שמחוץ לגבולות המדינה או מהם;

(3)

כללי התנהגות ואתיקה לבעלים, למחזיקים או למנהלים של מאגרי מידע ולעובדיהם;

(4)

הוראות לענין ביעור מידע עם הפסקת פעולתו של מאגר מידע.

אגרות

36א. (א)

שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, רשאי לקבוע–

(1)

אגרות בעבור רישום מאגר מידע ועיון בו לפי חוק זה;

(2)

אגרה, לתקופה שיקבע, בעבור מאגר מידע הרשום בפנקס (להלן – אגרה תקופתית), למעט מאגר מידע שבבעלות המדינה, ורשאי הוא לקבוע שיעורים שונים של אגרות תקופתיות לפי סוגים של מאגרים, וכן את מועדי התשלום של האגרה התקופתית, ותוספת אגרה לאגרה תקופתית שלא שולמה במועדה.

(ב)

כספי אגרות שנגבו לפי סעיף זה ייועדו לרשם וליחידת הפיקוח לצורך פעולתם לפי חוק זה.

(ג)

לא שולמה האגרה התקופתית או תוספת האגרה לאגרה התקופתית, לפי הענין, בתוך שישה חודשים מהמועד שנקבע בתקנות לתשלום תוספת האגרה, יותלה רישומו של המאגר בפנקס עד לתשלום.

תחילה

37.

תחילתו של פרק ב' ששה חדשים מיום פרסומו של חוק זה.

נספח ב'

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

בתוקף סמכותי לפי סעיף 36 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק או חוק הגנת הפרטיות), ובאישור ועדת חוקה חוק ומשפט של הכנסת, אני מתקינה תקנות אלה:

22.1. הגדרות

1.

בתקנות אלה–

"אירוע אבטחה חמור – "כל אחד מאלה:

(1)

במאגר מידע שחלה עליו רמת אבטחה גבוהה – אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע;

(2)

במאגר מידע שחלה עליו רמת אבטחה בינונית – אירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר;

"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;

"התקן נייד – "אחד מאלה:

(1)

מחשב המיועד לשימוש נייד לרבות מחשב שהוא ציוד קצה רט"ן כהגדרתו בפקודת הטלגרף האלחוטי [נוסח חדש], התשל"ב-1972;

(2)

מצא אחר המשמש לאחסון חומר מחשב;

"חומר מחשב "ו"מחשב – "כהגדרתו בחוק המחשבים, התשנ"ה-1995;

"מאגר המנוהל בידי יחיד – "מאגר מידע שמנהל יחיד או תאגיד בבעלות יחיד, ואשר רק היחיד ולכל היותר שני בעלי הרשאה נוספים רשאים לעשות בו שימוש ובאפשרותם לעשות בו שימוש, ולמעט מאגרי מידע כמפורט להלן:

(1)

מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר;

(2)

מאגר מידע שיש בו מידע על אודות 10,000 אנשים ומעלה;

(3)

מאגר מידע הכולל מידע שבעל המאגר כפוף בשלו לחובת סודיות מקצועית לפי דין או לפי עקרונות של אתיקה מקצועית;

"מאגרים שחלה עליהם רמת האבטחה הבסיסית – "מאגרי מידע שאינם מן הסוגים המפורטים בתוספת הראשונה או השנייה ואינם מאגר המנוהל בידי יחיד;

"מאגרים שחלה עליהם רמת האבטחה הבינונית – "מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה ואינם מאגר המנוהל בידי יחיד;

"מאגרים שחלה עליהם רמת האבטחה הגבוהה – "מאגרי מידע מן הסוגים המפורטים בתוספת השנייה;

"מידע ביומטרי – "מידע המשמש לזיהוי אדם, שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת;

"ממונה על אבטחה – "כמשמעותו בסעיף 17ב לחוק;

"מערכות המאגר – "מערכות המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע;

"נושא המידע – "האדם שעל אודותיו קיים מידע במאגר המידע;

"הרשות הלאומית להגנת הסייבר – "הרשות הלאומית להגנת הסייבר שייעודה הגנה על מרחב הסייבר, שהוקמה על פי החלטת הממשלה ופועלת בהתאם להחלטותיה;

"רשת ציבורית – "רשת תקשורת המאפשרת שימוש גם על ידי מי שאינו בעל הרשאה.

22.2. מסמך הגדרות המאגר

.2א

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.

(ב)

בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד 31 בדצמבר.

(ג)

בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

22.3. ממונה על אבטחת מידע

3.

חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה:

(1)

ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר;

(2)

הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר;

(3)

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

(4)

הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;

(5)

הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות בפסקאות (2) ו-(3), לשם ביצוע תקנות אלה, יגדירן בצורה ברורה;

(6)

בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.

22.4. נוהל אבטחה

4 (א)

בעל מאגר המידע יקבע במסמך נוהל אבטחת מידע (להלן – נוהל האבטחה) בהתאם למסמך הגדרות המאגר ותקנות אלה, אשר יחייב כל בעל הרשאה בהתאם לפרטים מהנוהל שאליו הוא חשוף לפי תקנת משנה (ב).

(ב)

בעל מאגר מידע ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

(ג)

נוהל האבטחה יכלול, בין השאר, את כל אלה:

(1)

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

(2)

הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8;

(3)

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

(4)

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

(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;

(6)

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

(7)

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

(ד)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, נוסף על האמור בתקנת משנה (ג), התייחסות גם לכל אלה:

(1)

אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9;

(2)

אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10;

(3)

הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16;

(4)

הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א);(1)

(5)

הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר.

(ה)

בעל מאגר מידע יבחן, אחת לשנה, את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור, יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה:

(1)

נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע;

(2)

נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

(ו)

ארגון שהוא בעל כמה מאגרי מידע רשאי לקבוע נוהל אבטחה כאמור בתקנה זו, במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.

22.5. מיפוי מערכות המאגר וביצוע סקר סיכונים

5 (א)

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.

(ב)

המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

(ג)

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן – סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.

(ד)

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו.

(ה)

ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי כאמור בתקנת משנה (א), במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה וכן רשאי לקיים את החובות הקבועות בתקנות משנה (ג) ו-(ד) בסקר סיכונים או במבדק חדירות, לפי העניין, אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה.

22.6. אבטחה פיזית וסביבתית

.6(א)

בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

(ב)

בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.

22.7. אבטחת מידע בניהול כוח אדם

7(א)

לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו הנוגע בדבר, כאמור בתקנה 8.

(ב)

בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם, יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע על אודות חובותיהם לפי החוק ונוהל האבטחה.

(ג)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש – סמוך ככל האפשר למועד תחילת הסמכתו.

22.8. ניהול הרשאות גישה

8(א)

בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

(ב)

בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).

22.9. זיהוי ואימות

9(א)

בעל מאגר מידע ינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות.

(ב)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה–

(1)

אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה;

(2)

ייקבעו בנוהל האבטחה גם הוראות לעניין תקנת משנה (א), ובכללן בנושאים אלה:

(א)

אופן הזיהוי; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על שישה חודשים;

(ב)

ניתוק אוטומטי לאחר פרק זמן של אי-פעילות;

(ג)

אופן הטיפול בתקלות הקשורות באימות זהות.

(ג)

בעל מאגר מידע ידאג לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

22.10. בקרה ותיעוד גישה

10(א)

במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

)ב (

מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

)ג (

בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

)ד (

נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

)ה (

בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

22.11. תיעוד של אירועי אבטחה

) .11א (

בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן – אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

)ב (

בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

)ג (

במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.

)ד (

אירע אירוע אבטחה חמור–

(1)

יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע;

(2)

רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

22.12. התקנים ניידים

12.

בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.

22.13. ניהול מאובטח ומעודכן של מערכות המאגר

) .13א (

בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלת מערכות כאלה.

)ב (

בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.

)ג (

בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

22.14. אבטחת תקשורת

) .14א (

בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

)ב (

העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

)ג (

במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.

22.15. מיקור חוץ

) .15א (

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 ההתקשרות;

)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)

)ב (

ארגון שהוא בעל כמה מאגרי מידע, המתקשר עם גורם חיצוני לצורך מתן שירות הכרוך בגישה אליהם בידי הגורם החיצוני, רשאי לקיים את הוראות תקנת משנה (א)(2) בהסכם אחד לעניין כל מאגרי המידע ובלבד שהם באותה רמת אבטחה.

)ג (

תקנה זו לא תחול על התקשרות של בעל מאגר עם יחיד.

22.16. ביקורות תקופתיות

) .16א (

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר אחראי לכך שתיערך, אחת ל-24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.

)ב (

בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

)ג (

בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

)ד (

בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת עריכת סקר סיכונים שמתקיים בו האמור בתקנת משנה (ב).

)ה (

ארגון שהוא בעל כמה מאגרי מידע, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת ביקורת אחת לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.

22.17. שמירת נתוני אבטחה

) .17א (

בעל מאגר מידע ישמור את הנתונים הנצברים במסגרת יישום הוראות תקנות 6(ב), 8 עד 11, 14, 15(א)(4) ו-16, ככל שתקנות אלה חלות עליו, באופן מאובטח למשך 24 חודשים.

)ב (

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר יגבה את הנתונים שנשמרו כאמור בתקנת משנה (א), באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי.

22.18. גיבוי ושחזור של נתוני אבטחה

) .18א (

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר במסמך–

(1)

נהלים לביצוע גיבוי כאמור בתקנה 17(ב), באופן תקופתי שגרתי;

(2)

נהלים, להבטחת שחזור הנתונים כאמור בתקנה 17(ב), ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;

(3)

כי במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתעודו גם הליכי שחזור המידע, ובכלל זה – זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

)ב (

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל מאגר אחראי לכך שיישמר עותק הגיבוי של הנתונים האמורים בתקנה (א)(1) ושל הנהלים כאמור בתקנת משנה (א)(2), באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אבדן או הרס.

22.19. חובות בעל מאגר חלות על מנהל מאגר ומחזיק בו ותיעוד ביצוע פעולה

) .19א (

החובות החלות בתקנות אלה על בעל מאגר מידע, יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 2 ו-15(א) – הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.

)ב (

מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה שאינה יצירת מסמך, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין; הרשם רשאי לתת הוראות לעניין אופן תיעוד כאמור.

22.20. סמכויות הרשם

(1) (א)20.

הרשם רשאי, אם ראה כי קיימים טעמים שמצדיקים זאת, לפטור מאגר מסוים מחובות אבטחת מידע לפי תקנות אלה, או להחיל על מאגר מסוים חובות לפי תקנות אלה, כולן או חלקן, לפי נסיבות העניין, ובין השאר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר בעלי ההרשאות בו.

(2)

פטור מחובות או החלת חובות לפי פסקה (1) ייעשה בהודעה בכתב לבעל המאגר; בהודעה כאמור יקבע הרשם את המועד לתחילת הפטור או ההחלה, לפי העניין, ויכול שיקבע מועדים שונים לעניין תקנות שונות.

)ב (

הרשם רשאי להורות כי מי שיעמוד בהוראות מסמך מנחה בעניין אבטחת מידע או בהנחיות של רשות מוסמכת בעניין אבטחת מידע החלות עליו, יראו אותו כמקיים הוראות תקנות אלה, כולן או חלקן, אם השתכנע כי עמידה בהוראות המסמך המנחה בעניין אבטחת מידע או בהנחיות הרשות המוסמכת, לפי העניין, באופן שהורה לפי תקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע; לעניין זה–

"רשות מוסמכת – "גוף ציבורי המוסמך על פי דין לתת הנחיות בעניין אבטחת מידע;

"מסמך מנחה בעניין אבטחת מידע – "תקן רשמי, תקן ישראלי או תקן בין-לאומי כמשמעותם בחוק התקנים, התשי"ג-1953, או מסמך ייחוס, שהרשם אישר לעניין זה.

22.21. תחולה וסייגים לתחולה

21.

בתקנות אלה–

(1)

על מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה – יחולו תקנות 1 עד 20;

(2)

על מאגרי מידע שחלה עליהם רמת האבטחה הבינונית – יחולו תקנות 1 עד 4, 5(א), (ב) ו-(ה), 6 עד 15, 16(א), (ב), (ג) ו-(ה), 17, 18(א), 19 ו-20;

(3)

על מאגרים שחלה עליהם רמת האבטחה הבסיסית – יחולו תקנות 1 עד 3, 4(א), (ב), (ג), (ה) ו-(ו), 5(א), (ב) ו-(ה), 6(א), 7(א) ו-(ב), 8, 9(א) ו-(ג), 11(א) ו-(ב), 12 עד 15, 17, 19 ו-20;

(4)

על מאגר המנוהל בידי יחיד – יחולו תקנות 1, 2, 6(א), 9(א), 11(א), 12 עד 14 ו-20.

22.22. תחילה

22.

תחילתן של תקנות אלה שנה מיום פרסומן.

22.23. הוראת מעבר

23.

על אף האמור בתקנה 7(א), בנוגע למי שהם בעלי הרשאות ביום תחילתן של תקנות אלה, בעל מאגר שחלה עליו התקנה האמורה יבחן את מידת התאמתם לגישה למאגר מידע באמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם, וכל זאת בשים לב לרגישות המידע ולסוג הרשאת הגישה ויעדכן בהתאם לצורך את הרשאות הגישה.

22.24. ביטול

24.

תקנות 2, 3, 9, 10, 12, 13, 14 ו-15 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 – בטלות.

22.25. יחס לחיקוקים אחרים

25.

תקנות אלה יחולו נוסף על הוראות בעניין אבטחת מידע בחיקוקים אחרים, זולת אם יש סתירה ביניהם.

תוספת ראשונה

)תקנה 1 והתוספת השנייה(

1.

מאגרי מידע שחלה עליהם רמת האבטחה הבינונית–

(1)

מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר;

(2)

מאגר מידע שבעליו הוא גוף ציבורי כמשמעותו בסעיף 23 לחוק, אף אם לא התקיימו בו הוראות פסקה (1) או;(3)

(3)

מאגר מידע הכולל מידע שהוא אחד מאלה:

)א (

מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד;

)ב (

מידע רפואי או מידע על מצבו הנפשי של אדם;

)ג (

מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000;

)ד (

מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם;

)ה (

מידע על אודות עברו הפלילי של אדם;

)ו (

נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007;

)ז (

מידע ביומטרי;

)ח (

מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם;

)ט (

הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים (א) עד (ז) או על אישיותו של אדם, אמונתו או דעותיו.

2.

על אף האמור בפרט 1(3), על מאגר מידע המקיים אחד מאלה, לא חלה רמת האבטחה הבינונית אלא רמת האבטחה הבסיסית:

(1)

המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ה), (ו), (ז) לעניין תמונות פנים בלבד ו-(ח), על אודות המועסקים או הספקים של בעל מאגר המידע, ובלבד שהמידע משמש למטרות ניהול העסק בלבד, ואינו כולל מידע מן הסוגים המפורטים בפרט 1(3)(א), (ג), (ד) ו-(ז) לעניין מידע שאינו תמונות פנים ו-(ט);

(2)

מספר בעלי ההרשאה אצל בעל המאגר אינו עולה על עשרה.

תוספת שנייה

)תקנה 1(

מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה–

(1)

מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה, לרבות מאגר של גוף ציבורי כמשמעותו בסעיף 23(1) לחוק המקיים את האמור בפרטים (1) או (3), שיש בו מידע על אודות 100,000 אנשים ומעלה;

(2)

מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה, לרבות מאגר של גוף ציבורי כמשמעותו בסעיף 23(1) לחוק המקיים את האמור בפרטים (1) או (3), שמספר בעלי ההרשאה בו עולה על 100.

נספח ג'

תקציר מדוח מבקר המדינה "אבטחת מידע והגנת הפרטיות ברשויות המקומיות (מעקב מורחב) - דוח על הביקורת בשלטון המקומי התשע"ז - 2017

רקע כללי

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה - הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק), קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק מגדיר, בין היתר, "מידע" כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו", ו"מאגר מידע" כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב". עוד קובע החוק כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

ברשויות המקומיות מאגרי מידע רבים המשמשים בסיס לעבודתן בעתות רגיעה וחירום, בין היתר בתחומים האלה: כספים, תכנון ובנייה, חינוך, רווחה, כוח אדם, רישוי עסקים, תחבורה וחניה, תברואה. בשנים האחרונות אף גדל מספר הערים החכמות - ערים המשתמשות בטכנולוגיות מידע ותקשורת לשיפור ניהול נכסיהן ואיכות החיים של תושביהן. מגמה זו מביאה לגידול חד בכמות הנתונים שבידי הרשויות המקומיות ובמספר מאגרי המידע שבבעלותן. פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, כמו פגיעה בשירותים הניתנים לתושב ובצנעת הפרט, ולכן מוטלת עליהן החובה להגן על המידע.

בדוח בנושא אבטחת מידע והגנת הפרטיות ברשויות המקומיות שפרסם מבקר המדינה במאי 2012[51] (להלן - הביקורת הקודמת) הועלו ליקויים רבים הן במישור המאסדרים בתחום זה - הרשות למשפט, טכנולוגיה ומידע (להלן - רמו"ט), שהוקמה במשרד המשפטים בספטמבר 2006 כרשות להגנת מידע אישי בישראל, והמינהל לשלטון מקומי במשרד הפנים - והן במישור הרשויות המקומיות[52].

51 מבקר המדינה, **דוח ביקורת שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות מקומיות", עמ' 1513-1537.

52 הרשויות המקומיות שנבדקו בביקורת הקודמת הן: עיריות אשקלון, בני ברק, טירה, יהוד-מונוסון ויקנעם עילית והמועצות המקומיות בני עי"ש ורמת ישי.

פעולות הביקורת

בחודשים אוקטובר 2016 - ינואר 2017 עשה מבקר המדינה ביקורת בנושא אבטחת המידע והגנת הפרטיות ברשויות המקומיות (להלן - הביקורת הנוכחית). הביקורת הנוכחית כללה גם מעקב אחר אופן תיקון הליקויים שהועלו בביקורת הקודמת בפעולותיהם של עיריות יהוד-מונוסון ויקנעם עילית, רמו"ט ומשרד הפנים בנושא האמור. כמו כן נבדקו פעולותיהן בנושא של חמש רשויות מקומיות נוספות שלא נכללו בביקורת הקודמת - עיריות באר שבע, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון (להלן - הרשויות המקומיות הנוספות שנבדקו). בדיקות השלמה נעשו ברשות הלאומית להגנת הסייבר במשרד ראש הממשלה.

הליקויים העיקריים

אסדרת הטיפול בנושא אבטחת מידע והגנת הפרטיות

הצוותים לתיקון הליקויים של משרד הפנים ושל משרד המשפטים לא דנו בממצאי הביקורת הקודמת על פעולות המינהל לשלטון מקומי ורמו"ט, בהתאמה, שלא כנדרש בחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ולא פעלו לתיקון הליקויים שהועלו בה.

היערכות משרד הפנים לאיומי סייבר[53] נמצאת רק בראשית דרכה, וטרם הוקם גוף שיפקח על היערכותן של הרשויות המקומיות לאיומי סייבר וינחה את הרשויות בתחום זה כמתחייב מהחלטת ממשלה 2443 מפברואר 2015 בה נקבע כי משרדי הממשלה, שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר, יקדמו את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים.

פעילות הרשויות המקומיות בתחום אבטחת מידע והגנת הפרטיות עדיין אינה מאוסדרת על ידי השלטון המרכזי. המינהל לשלטון מקומי במשרד הפנים ורמו"ט שבמשרד המשפטים ממשיכים להטיל זה על זה את האחריות לאסדרת הנושא. כתוצאה, כל רשות מקומית מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי בנושא.

אבטחת המידע הממוחשב ברשויות המקומיות

רישום מאגרי מידע: עיריית כרמיאל והמועצה המקומית תל מונד לא רשמו את מאגרי המידע שלהן אצל רשם מאגרי המידע ברמו"ט; עיריות יקנעם עילית

53 בהחלטת ממשלה 3611 מ-7.8.11 הוגדר מרחב הסייבר כ"המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".

ונצרת עילית רשמו רק חלק ממאגרי המידע שלהן; וועדים מקומיים[54] במועצה האזורית הגליל התחתון לא רשמו את מאגרי המידע שלהם.

מינוי ממונה על אבטחת מידע: משרד הפנים לא בחן אם יש להחיל על הרשויות המקומיות את הוראות החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, ולפיהן ממוני הביטחון מופקדים על הפעולות לאבטחת מידע ומערכות המידע, אף שנדרש לעשות כן בביקורת הקודמת; בקובץ תיאורי התפקיד[55] שפרסם משרד הפנים נקבע, שלא בדומה להמלצות למשרדי הממשלה המפורטות בנוהלי המסגרת לאבטחת מידע[56] (להלן - נוהלי המסגרת), כי מנהל אבטחת המידע ברשות מקומית יהיה כפוף למנהל מערכות המידע הראשי שלה.

נהלים והנחיות לאבטחת מידע: עיריות כרמיאל ונצרת עילית והמועצה המקומית תל מונד לא קבעו נהלים, הנחיות וכללים מחייבים לאבטחת המידע. כל הרשויות המקומיות שנבדקו אינן מנהלות רישום מעודכן של הרשאות הגישה למאגרי המידע שניתנו לכל אחד מעובדיהן.

בקרה ופיקוח לוגיים[57]: כל הרשויות המקומיות שנבדקו אינן מבצעות ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות אשר גורמים בלתי מורשים ביצעו או ניסו לבצע.

אבטחת חומרה: חדרי המחשב של עיריות יהוד-מונוסון, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון אינם עומדים בדרישות התקן הישראלי בנושא בטיחות אש של מחשבים וציוד היקפי.

סקרי סיכונים ובדיקות חדירה: עיריות כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון לא ביצעו מעולם סקרי סיכונים ומבחני חדירה כדי להעריך את הסיכונים הנשקפים למאגרי המידע שברשותן ואת הנזק העלול להיגרם למערכות המידע שלהן.

אירועי אבטחת מידע: אף שבשנים האחרונות גדל היקף התקיפות באמצעות נוזקות (malware)[58] שונות, והפרות החוק ו"פשיעת המידע" הולכות ומתרבות, אין בידי שום גורם תמונת מצב עדכנית על היקף התופעה ברשויות המקומיות, זאת בשל היעדר חובת דיווח על פגיעות מסוג זה. למשל, עיריות יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית הותקפו לפחות פעם אחת על ידי נוזקה מסוג כופרה (ransomware)[59]. בעיריית נצרת עילית נפגע השרת במחלקת ההנדסה,

54 הוועדים המקומיים בית קשת, בית רימון, גבעת אבני, הזורעים, מצפה נטופה ושרונה.

55 משרד הפנים, מינהל השלטון המקומי, האגף לכוח אדם ושכר ברשויות המקומיות, **קובץ ניתוח העיסוקים ותיאורי התפקידים ברשויות המקומיות** (ספטמבר 2011).

56 משרד ראש הממשלה, אגף בכיר לביקורת המדינה והביקורת הפנימית, המועצה המייעצת לביקורת ואבטחת מידע, **נוהלי מסגרת לאבטחת מידע**, מהדורה שלישית (ספטמבר 2005).

57 בקרה לוגית - ניטור ממוחשב שוטף של הפעילות במערכת הממוחשבת תוך התמקדות באירועים חריגים או רגישים; פיקוח לוגי - מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות.

58 תוכנה שמטרתה לחדור למחשב או להזיק לו ללא ידיעתו של המשתמש בו. הגדרה זו חלה על וירוסים, תולעי מחשבים, רוגלות (תוכנות ריגול), סוסים טרויאניים ותוכנות פרסום.

59 נוזקה המגבילה את הגישה לנתונים השמורים במערכת המחשב ומשמשת לסחוט מהמשתמש תשלום (דמי כופר) על מנת שתוסר מגבלת הגישה למערכת.

ולמועד סיום הביקורת, ינואר 2017, הקבצים השמורים בשרת נשארו מוצפנים ולעירייה לא הייתה גישה אליהם.

התקשרויות עם חברות פרטיות המחזיקות במאגרי מידע של הרשות המקומית

רשם מאגרי המידע ברמו"ט אינו אוכף על חברות פרטיות המחזיקות במאגרי מידע של רשויות מקומיות את חובת הדיווח השנתי על מאגרי המידע שהן מחזיקות בהם כנדרש בחוק.

לעיריית כרמיאל אין חוזים למתן שירותים עם כל החברות הפרטיות המחזיקות במאגרי המידע שלה.

הדרכה וביקורת בתחום אבטחת מידע והגנת הפרטיות ברשויות המקומיות

כל הרשויות המקומיות שנבדקו לא קבעו תכנית הדרכה והסברה שנתית לעובדים בתחום אבטחת המידע והגנת הפרטיות.

בשנים 2006-2016 לא בוצעו ביקורות פנימיות בנושא אבטחת מידע והגנת הפרטיות בעיריית כרמיאל, במועצה המקומית תל מונד ובמועצה האזורית גליל תחתון.

האגף לביקורת ברשויות המקומיות של משרד הפנים אינו מבצע ביקורת בנושא אבטחת מידע והגנת הפרטיות במסגרת הביקורת השנתית של רואי החשבון המבקרים.

ההמלצות העיקריות

על משרד הפנים לפרסם בקרב הרשויות המקומיות קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות. על ההנחיות לעסוק בחובת הרישום של מאגרי מידע - ובכלל זה בחובת הרישום החלה על ועדים מקומיים, ובנושאי האבטחה הלוגית והפיזית, בחובת הדיווח על אירועי אבטחת מידע ועל הפעולות שננקטו בעקבותיהם ובחובה לקיים פעולות הדרכה והסברה בתחום אבטחת המידע, בדומה להמלצות המפורטות בנוהלי המסגרת. על המשרד להקים בהקדם גוף מנחה ומפקח בתחום ההיערכות לאיומי סייבר מול הרשויות המקומיות כמתחייב מהחלטת ממשלה 2443 מפברואר 2015.

נוכח מספרם הרב של מאגרי מידע בבעלות רשויות מקומיות שאינם רשומים אצל רשם מאגרי המידע, על רמו"ט לבחון את הפעולות הנדרשות לאסדרת הנושא ולאכוף את הוראות החוק.

על הרשויות המקומיות לרשום את כל מאגרי המידע שלהן; לבצע סקרי סיכונים ובדיקות חדירות; לבצע בקרה ופיקוח לוגיים על הפעולות המתבצעות במאגרי המידע שבבעלותן; לאבטח את חדרי המחשב שלהן ולהתאימם לדרישות התקן הישראלי בנושא בטיחות אש של מחשבים וציוד היקפי; לגבש וליישם תכנית הדרכה והסברה לעובדים; ולכלול בתכניות הביקורת של מבקרי הפנים שלהן ביקורת בנושא אבטחת מידע והגנת הפרטיות.

סיכום

במסגרת פעילותן השוטפת של הרשויות המקומיות נעשה שימוש רב במאגרי מידע הכוללים נתונים אישיים רבים על התושבים. ככל שהן מרבות להשתמש במאגרי מידע גוברת הסכנה שהמידע ייחשף ברבים ותיפגע פרטיותם של התושבים. לכן מוטלת על הרשויות המקומיות החובה להגן על מידע זה ולהגביר את חסינותן הן בפני דליפת מידע והן לצורכי הגנה על רציפות תפקודית לטובת השירות לציבור.

בשנים האחרונות גדל היקף התקיפות של מערכות המחשוב של גופים רבים באמצעות כופרות המגבילות גישה למערכות המחשב, שנועדו לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה או באמצעות נוזקות המאפשרות לאדם שאינו מוסמך לכך להעתיק את הנתונים השמורים בהן. ההיקף הכולל של התופעה ברשויות מקומיות אינו ידוע, בהיעדר חובה לדווח על תקיפות מסוג זה.

ממצאי הביקורת מלמדים כי במועד סיום הביקורת הנוכחית, כחמש שנים לאחר שבוצעה הביקורת הקודמת, משרד הפנים ומשרד המשפטים עדיין מטילים זה על זה את האחריות לאסדרת הנושא, ולמותר לציין שהם לא פעלו לתיקון הליקויים שהועלו בביקורת הקודמת, והדבר פוגע ברמת אבטחת המידע בשלטון המקומי. עוד מעידים ממצאי הביקורת כי כל רשות מקומית עדיין מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי באבטחת המידע שלהן ובהגנה על הפרטיות של תושביהן.

נוכח האמור לעיל, על מנכ"ל משרד הפנים ומנכ"לית משרד המשפטים לגבש מתכונת ברורה של חלוקת תחומי האחריות והסמכויות בין משרדיהם בכל הנוגע לאבטחת המידע והגנת הפרטיות ברשויות המקומיות, ולפעול למימושה של מתכונת זו.

על הרשויות המקומיות לתקן את הליקויים שהועלו בדוח בנוגע לפעולותיהן בתחום אבטחת המידע והגנת הפרטיות, לפעול להעלאת המודעות בקרב עובדיהן לחשיבות הנושא ולהעמיד לרשות העובדים את האמצעים למילוי חובותיהם בתחום זה.

נספח ד'

תקציר מדוח מבקר המדינה "ניהול מערכות מידע ברשויות המקומיות" - דוח על הביקורת בשלטון המקומי התשפ"ב-2022

רקע

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים לצורך בסיסי ומחויב המציאות. בכלל זה, בין היתר, נעשה שימוש במאגרי מידע הכוללים נתונים אישיים על התושבים ועל הגורמים המקיימים קשר עם הרשויות במגוון תחומים. ברשויות המקומיות מצטבר מידע אישי על תושביהן, כמו שם, כתובת, מספר זהות, מספר טלפון, מידע רפואי, מידע בתחומי רווחה ונתונים על אמצעי התשלום שהם בוחרים לשלם באמצעותם וכן מידע בלתי מסונן כמו לוחיות רישוי, תווי פנים, נתוני מיקום והרגלי תנועה. רשויות מקומיות מתמודדות עם מגוון סיכונים, ובכלל זה עם פרצות במערך אבטחת המידע ועם איומי סייבר, ומערכות המידע שלהן הפכו למוקד של עניין עבור פצחנים (האקרים) ופושעי סייבר. מכאן נובע הצורך לשמור על מערכות המידע למניעת פגיעה ברציפות התפקודית של הרשויות המקומיות במתן שירותים וכן למניעת דליפה של נתונים ומידע ממאגרי המידע שברשותן ולמניעת חשיפתם לגורמים שאינם מורשים לכך.

נתוני מפתח

67%	61%	108	41%
שיעור הרשויות המקומיות (87 מ-130) שקיבלו ציון חוסן קיברנטי נמוך מ-60	שיעור הרשויות המקומיות שאין להן תוכנית להתאוששות מאסון בהתרחש	מספר הפניות המצטבר שהתקבלו מ-32 רשויות מקומיות בשנים	שיעור הרשויות המקומיות שחוו אירועי סייבר (בפועל או ניסיונות שלא צלחו)

במבדק שביצע אגף הסייבר במשרד הפנים	אירוע סייבר - BCP/DRP (36 מ-59 הרשויות שהשיבו על השאלה בעניין זה בשאלון)	2019 - 2021 במרכז לניהול אירועי סייבר (של מערך הסייבר הלאומי)	בשנים 2019 - 2021 (24 מ-59 הרשויות שהשיבו על השאלה בשאלון)
34%	64%	18%	49%
שיעור הרשויות המקומיות שאין להן ממונה או מנהל אבטחת מידע (21 מ-61 הרשויות שהשיבו על השאלה)	שיעור הרשויות המקומיות שאין להן נוהל אבטחת מידע (37 מ-58 הרשויות שהשיבו על השאלה בעניין זה בשאלון)	שיעור הרשויות המקומיות שלא מינו מנהל מערכות מידע ראשי (מנמ"ר) (11 מ-61 הרשויות שהשיבו על השאלון)	שיעור הרשויות המקומיות שלא ביצעו מבדקי חדירה בשנים 2019 - 2021 (30 מ-61 הרשויות שהשיבו לשאלון)

פעולות הביקורת

בחודשים יולי-נובמבר 2021 בדק משרד מבקר המדינה את נושא ניהול מערכות המידע ברשויות המקומיות. הבדיקה נעשתה בשמונה רשויות מקומיות שנבחרו, תוך מתן ביטוי למחוזות המינהליים שבהם שוכנות הרשויות; למעמדן המוניציפלי; ולמדד החברתי-כלכלי שאליו הן משויכות; למדד הפריפריאליות שאליו הן משויכות; למגזר שאליו רוב תושביהן משתייכים; ולמספר התושבים המתגוררים בתחום שיפוטן: בחמש עיריות - **חיפה, יוקנעם, נתיבות, ראש העין ושפרעם**; בשתי מועצות מקומיות - **גדרה ועין מאהל**; ובמועצה האזורית **מטה בנימין** (להלן - הרשויות שנבדקו). בדיקות השלמה נעשו במשרד הפנים -

במינהל שירותי חירום ובמפעם עמק יזרעאל, במרכז השלטון המקומי ובמערך הסייבר הלאומי שבמשרד ראש הממשלה (להלן - מערך הסייבר). כמו כן במסגרת הבדיקה נשלחו שאלונים ל-63 רשויות מקומיות, ו-61 (97%) מהרשויות שנדגמו השיבו עליהם.

לפי החוק אסור לפרסם את הדו"ח לפני שחלף המועד שנקבע להגשתו למועצה..

המפרסם דו"ח בניגוד לדין, דינו – מאסר שנה. תחום אבטחת מידע – חסוי ברובו גם בהמשך

תמונות מצב העולה מהביקורת

מבדקים שביצע אגף הסייבר במשרד הפנים - עלה כי אגף הסייבר במשרד הפנים השלים מבדק בסיסי ב-130 מ-257 רשויות, נכון לאוגוסט 2021. עוד עלה כי 87 (כ-67%) מ-130 הרשויות קיבלו ציון הנמוך מ-60, ואילו רק 11 (כ-8%) מהרשויות קיבלו ציון הגבוה מ-80, והציון הממוצע היה 48. עולה אפוא מהנתונים כי רמת אבטחת המידע והמוכנות של מרבית הרשויות המקומיות (67% מהן) לאיומי סייבר היא נמוכה, וכי הרשויות השונות שבחן משרד הפנים נבדלות זו מזו במידה רבה מבחינת מוכנותן לאירועי סייבר.

דיווחים למרכז הארצי לניהול אירועי סייבר (של מערך הסייבר) - מנתוני מערך הסייבר בנוגע לפניות של רשויות מקומיות למרכז לניהול אירועי סייבר עלה כי בשנת 2019 פנו למרכז 14 רשויות ב-32 פניות, בשנת 2020 פנו למרכז 25 רשויות ב-40 פניות, ובשנת 2021 פנו למרכז 19 רשויות ב-36 פניות. בסך הכול בשנים 2019 - 2021 פנו במצטבר 32 רשויות מקומיות (מתוך 257) ב-108 פניות.

הגדרת תחומי האחריות בין משרד הפנים למערך הסייבר - משרד הפנים ומערך הסייבר לא השלימו את הסדרת הסמכויות החסרות בכל הנוגע לרגולציה ולהנחיה מקצועית של הרשויות המקומיות בתחומי אבטחת מידע והגנת הפרטיות. בתוך כך, משרד הפנים לא פעל להכנת נוהל שמטרתו להנחות את הרשויות המקומיות כיצד לפעול בנושא. כפועל יוצא, נכון למועד סיום הביקורת אין לרשויות המקומיות גורם מאסדר בתחום אבטחת המידע והגנה מאיומי סייבר, ומזה שנים הרשויות המקומיות פועלות ללא הנחיות מקצועיות ברורות בנושא וכל רשות מקומית פועלת בעניין לפי ראות עיניה.

תוכניות עבודה בנושא מערכות מידע - הרשויות המקומיות **גדרה**, **יוקנעם**, **מטה בנימין**, **נתיבות**, **עין מאהל ושפרעם** לא הכינו תוכניות עבודה אסטרטגיות רב-שנתיות בנושא מערכות המידע, ולא הכינו תוכניות עבודה שנתיות מקושרות תקציב בהתאם ליעדי הרשות המקומית לטווח הארוך. עוד נמצא כי עיריות **חיפה וראש העין**, אשר גיבשו תוכניות אסטרטגיות בנושא מערכות המידע, לא תקצבו אותן ומשכך התוכניות לא יושמו.

מינוי ממונה אבטחת מידע - 21 (כ-34%) מ-61 הרשויות שענו על שאלה בעניין זה בשאלון אינן מעסיקות ממונה אבטחת מידע כנדרש, ומבין הרשויות שנבדקו למועצות המקומיות **גדרה** ו**עין מאהל** אין ממונה אבטחת מידע.

נוהל אבטחת מידע - מבין הרשויות שנבדקו, רשויות א', ג' ו-ה' לא הכינו נוהל אבטחת מידע כנדרש בתקנות אבטחת המידע. רשויות ד', ו' ו-ח' הכינו רק טיוטה של הנוהל, ובמועד סיום הביקורת היא לא אושרה.

נוהל גיבויים ויישומו - נמצא כי מבין הרשויות שנבדקו, לרשויות א', ג', ד', ה' ו-ז' אין נוהל גיבויים כנדרש. לרשויות ו' ו-ח' יש טיוטות נוהל גיבויים שטרם אושרו. ברשויות ג', ד' ו-ח' לא נמצאו רישומים המתעדים היסטוריית גיבויים תקינה ברשות. **ניהול הרשאות גישה** - לרשויות ג', ד' ו-ה' אין כללים כתובים בנוגע למתן הרשאות גישה או לביטולן. לרשות א'

לפי החוק אסור לפרסם את הדו"ח לפני שחלף המועד שנקבע להגשתו למועצה..

המפרסם דו"ח בניגוד לדין, דינו – מאסר שנה. תחום אבטחת מידע – חסוי ברובו גם בהמשך

יש נוהל שנכנס לתוקף ביוני 2021, ולרשויות ו' ו-ח' יש טיוטות נוהל בנושא מיולי 2020 ומיולי 2021 בהתאמה, שלא אושרו במועד סיום הביקורת.

תוכנית להתאוששות מאסון בהתרחש אירוע סייבר - 36 (כ-61%) מהרשויות המקומיות שהשיבו על השאלה בנושא קיום תוכנית להתאוששות מאסון ציינו כי אין ברשות מנגנון מוסדר להמשכיות של פעילות המחשוב ברשות בהתרחש אירוע סייבר. הרשויות שנבדקו - א', ב', ג', ד', ה', ז' ו-ח' - לא הכינו כלל תוכנית להתאוששות מאסון. רשות ו' הכינה טיוטת תוכנית כאמור, ובמועד סיום הביקורת היא טרם אושרה.

סקרי סיכונים ומבדקי חדירה או ביקורות תקופתיות - רשות ה' ביצעה סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים) בשנת 2020 ולא ביצעה מבדקי חדירה במערכות המאגר (להלן מבדקי חדירה). רשות ו' ביצעה סקר סיכונים בשנת 2019 ולא ביצעה מבדקי חדירה. רשויות ג',ד' ו-ח', שאינן מחויבות בביצוע מבדקי חדירה, לא ביצעו כלל סקרי סיכונים או ביקורות תקופתיות. עוד הועלה כי רשות א' לא ביצעה בעצמה מבדק חדירה או סקר סיכונים אלא הסתמכה בעניין זה על החברה הפרטית המספקת לרשות שירותי מחשוב.

יש לציין לחיוב את רשויות ב', ו' ו-ז' על שביצעו מבדקי חדירה או סקרי סיכונים למיפוי הסיכונים ברשות בשנים 2019 - 2021.

עיקרי המלצות הביקורת

מומלץ כי משרד הפנים ומערך הסייבר יפעלו במשותף, תוך התחשבות בייחודיות של מגזר השלטון המקומי, לחלוקת הסמכויות ביניהם לשם יישום החלטת הממשלה 2443 בנוגע למגזר זה, באופן שיוסמך רגולטור מוביל להסדרת ההיערכות של הרשויות המקומיות לאיומי סייבר ולקביעת נהלים מתאימים שיסדירו את פעילות הרשויות המקומיות בנושא. עוד מומלץ למערך הסייבר לפעול בשיתוף אגף הסייבר במשרד הפנים להעלאת המודעות של הרשויות המקומיות לחשיבות הדיווח למרכז לניהול אירועי סייבר על אירועי סייבר שהן נחשפו להם ולאפשרות ההיוועצות עם מערך הסייבר.

על הרשויות המקומיות **גדרה**, **יוקנעם**, **מטה בנימין**, **נתיבות**, **עין מאהל ושפרעם** להכין תוכנית עבודה אסטרטגית שתשמש בסיס לתוכניות עבודה שנתיות ולהגישה להנהלת הרשות כדי שתדון בה, תבחן אם ניתן ליישמה במסגרת תקציבה ותפעל בהתאם ליישומה.

לאור החובה המוטלת על הרשויות המקומיות לאייש את תפקיד ממונה אבטחת המידע ברשות, על כלל הרשויות המקומיות, שלא מינו ממונה כאמור, וביניהן הרשויות המקומיות **גדרה ועין מאהל**, לפעול לאיוש התפקיד. מומלץ כי משרד הפנים ינחה את הרשויות שלא

לפי החוק אסור לפרסם את הדו"ח לפני שחלף המועד שנקבע להגשתו למועצה..

המפרסם דו"ח בניגוד לדין, דינו – מאסר שנה. תחום אבטחת מידע – חסוי ברובו גם בהמשך

מינו ממונה לעשות כן, וכן ישלים, בשיתוף מרכז השלטון המקומי, את הגדרת התפקיד של מנהל מערכות המידע הראשי (מנמ"ר) ואת תנאי העסקתו.

- על רשויות א', ג', ו-ה' להכין נוהל אבטחת מידע כנדרש. כמו כן על הרשות המקומית א' לפעול לאישור נוהל אבטחת המידע של חברה ב' ובמידת הצורך להתאימו לצורכי הרשות. על רשויות ד', ו' ו-ח' להשלים את אישור הנוהל ולציין בו את מועד כניסתו לתוקף.
- על רשויות א', ג', ד', ה', ו', ז' ו-ח' לקבוע נוהל גיבויים תקף ולבצע גיבויים על פי הנקבע בו.
- על רשויות ג', ד' ו-ה' לקבוע כללים למתן הרשאות ולביטולן, הן לעובדים הנקלטים ברשות והן לעובדים העוזבים אותה. על רשויות ו' ו-ח' לאשר את טיוטות הנוהל שלהן ולפעול על פיו.
- נוכח החשיבות של הכנת תוכנית להתאוששות מאסון, משרד מבקר המדינה ממליץ לכלל הרשויות המקומיות, ובהן הרשויות שנבדקו (רשויות א', ב', ג', ד', ה', ז' ו-ח'), לפעול להכנת תוכנית להתאוששות מאסון המתאימה לצורכי הרשות, בהתאם להנחיות מערך הסייבר. מומלץ כי רשות ו' תפעל להשלמת הכנתה של התוכנית להתאוששות מאסון.
- על רשויות ג', ד' ו-ח' לבצע ביקורות תקופתיות, רצוי במסגרת סקרי סיכונים, על מנת למפות ולאתר את סיכוני אבטחת המידע ברשות ולהיערך בהתאם לממצאים שיועלו. עוד מומלץ כי הרשויות ג', ד', ו' ו-ח' יבצעו מבדקי חדירה גם אם מאגרי המידע שלהן כפופים לרמת אבטחה בינונית.

לפי החוק אסור לפרסם את הדו"ח לפני שחלף המועד שנקבע להגשתו למועצה..

המפרסם דו"ח בניגוד לדין, דינו – מאסר שנה. תחום אבטחת מידע – חסוי ברובו גם בהמשך

התרשים בעיבוד משרד מבקר המדינה.

סיכום

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים לצורך בסיסי ומחויב המציאות, והוא חשוף לאיומי סייבר. נוסף על כך, במאגרי המידע של הרשויות המקומיות שמורים, בין היתר, נתונים אישיים על התושבים ועל הגורמים הבאים בקשר עם הרשויות במגוון תחומים, דבר המחייב נקיטת אמצעים לאבטחת המאגרים, גם לשם הגנה על הפרטיות.

ברשויות המקומיות שנבדקו הועלו ליקויים שונים בתחום הגנת הסייבר ואבטחת המידע, שמקורם, בין היתר, בהיעדר אסטרטגיה והכוונה מצד הגורמים האחראים בתחום. בשל חשיבות הנושא מומלץ כי אגף הסייבר במשרד הפנים בשיתוף מערך הסייבר הלאומי יפעלו להנחיית הרשויות המקומיות באופן שיבהיר מהן החובות החלות עליהן וכיצד ניתן לפעול באופן המיטבי לשיפור אבטחת המידע בהן. עוד מומלץ כי הרשויות המקומיות יפעלו באמצעות הכלים העומדים לרשותן לקביעת אסטרטגיה רשותית לניהול מערכות המידע שברשותן ולחיזוק אבטחת המידע בהן. על כלל הרשויות המקומיות לנקוט את כל האמצעים העומדים לרשותן לניהול מיטבי של מערכות המידע שלהן ולהגברת מוכנותן להגנה על המידע הרגיש הנמצא בבעלותן ולמניעת פגיעה ברציפות התפקודית שלהן.