



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

לכבוד

ערן דורון- ראש המועצה

מועצה אזורית רמת נגב

בהתאם לתוכנית הביקורת הפנימית של המועצה לשנת 2023, אני מתכבד להגיש לעיוןך את
דוח הביקורת בנושא הגנת הפרטיות- עמידה בתקנות

בכבוד רב,

דוד שטרק, ר"ח

מבקר המועצה וממונה על תלונות הציבור

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות

מועצה אזורית רמת הנגב

דוח ביקורת פנימית בנושא

הגנת הפרטיות- עמידה בתקנות

שנת 2023

הדוח נערך על ידי

מבקר המועצה וממונה על תלונות הציבור



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

א. תוכן

3	תוכן
4	רקע
5	מטרת הדוח, מתודולוגיה ומסגרת נורמטיבית
6	תקציר מנהלים- עיקרי הממצאים וההמלצות
9	דוח הביקורת המפורט בנושא הגנת הפרטיות- עמידה בתקנות
28	סיכום
28	תגובת ראש המועצה



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

ב. רקע

ב.1. הקדמה

במחלקות המועצה מנוהל מידע אישי רגיש, לרבות:

1. מחלקת הרווחה – נתוני מטופלים
2. מחלקת החינוך – נתוני קטינים
3. שפ"ח – נתוני קטינים מטופלים
4. מחלקת הגביה – נתוני תושבים
5. מחלקת משאבי אנוש ומחלקת השכר – פרטים אישיים אודות עובדים לרבות שכר ומאגר ביומטרי
6. המוקד העירוני – הקלטות של פניות תושבים

ללא התנהלות נאותה, מידע רגיש זה עלול להיחשף בפני גורמים שאינם רלוונטיים, ובכך לפגוע בבעלי הפרטים, פגיעה נפשית, גופנית או ממונית.

סעיף 2 בחוק הגנת הפרטיות מפורטים המקרים שבהם קיימת פגיעה בפרטיות. להלן המקרים שרלוונטיים לרשות מקומית:

- (7) הפרה של חובת סודיות שנקבעה בדיון לגבי עניניו הפרטיים של אדם;
- (8) הפרה של חובת סודיות לגבי עניניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;
- (9) שימוש בידעיה 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);

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

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

על מנת למנוע פגיעה בפרטיות, החוק התקנות וההנחיות (יפורטו בהמשך), קבעו את הדרך בה יש להתנהל עם מאגרי מידע המכילים פרטים אישיים.

ב.2. נתונים כלליים

לאחר שנעשה מיפוי של מערכות המידע במ.א רמת הנגב, ע"י גורם מקצועי. התברר כי למועצה ישנם 17 מאגרי מידע בנושאים שונים הקשורים לפעילות המועצה. המועצה מעסיקה חברה חיצונית שמלווה ומבקרת את פעילות מאגרי המידע

ג. מטרת הדוח, מתודולוגיה ומסגרת נורמטיבית

ג.1. מטרת הבדיקה כפי שנקבעו:

ביקשתי בדוח זה לבדוק את עמידת המועצה בתקנות הגנת הפרטיות.

ג.2. מתודולוגיה, זיהוי הסיכונים, פעולות והיקף הבדיקה-

במסגרת הביקורת נבדקו נושאים שונים להלן הפירוט:

- א. קיום מסמך הגדרות מאגר,
- ב. רישום מאגרי מידע,
- ג. מינוי ממנוה על אבטחת מידע,
- ד. קיום נהלי אבטחת מידע
- ה. מיפוי מערכות המאגר,
- ו. ביצוע סקרי סיכונים,
- ז. אבטחה פיזית וסביבתית,
- ח. ניהול הרשאות גישה וזיהוי ואימות,
- ט. הגבלת השימוש בהתקנים ניידים,
- י. בקרה ותיעוד גישה,
- יא. תיעוד של אירועי אבטחה,
- יב. הסכמים עם גורמים חיצוניים

ג.3. המסגרת הנורמטיבית

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

1. חוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "החוק").
2. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז, 2017 (להלן: "תקנות 2017").
3. תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו – 1986 (להלן: "תקנות 1986")
4. ¹הרשות להגנת הפרטיות פרסמה סדרת הנחיות מחייבות בנושא הגנת הפרטיות

ד. תקציר מנהלים- עיקרי הממצאים וההמלצות

ד.1. מפת הדוח

S



¹ ההנחיות מפורטות באתר של הרשות להגנת הפרטיות

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

ד.2. תקציר מנהלים- עיקרי ממצאים והמלצות

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

מס.	ממצאים	המלצות
1	בניגוד לסעיף 3 (4) בתקנות, המועצה מינתה את מנמ"ר המועצה לכהן כממונה על אבטחת המידע.	למנות מנהל אבט"מ CISO חיצוני מטעם חברת פריימסק שאיתה בוצע כל הליך האסדרה של אבטחת המידע
2	למועצה חסרה גישה למנגנון תיעוד אוטומטי שמאפשר בקרה על זהות המשמשים כנדרש בתקנות.	לדרוש מהחברות החיצוניות שמחזיקות בגישה לזהות המשתמשים שיהיה להם את המידע בזמינות יותר גבוהה
3	אין מספיק הדרכות בנושא אבטחת מידע בכלל והגנת הפרטיות בפרט	לבנות תכנית הדרכות מסודרת המחולקת מהן ההדרכות שצריך לעבור ומתי. ומעקב מי עבר אותם.
4	בניגוד תקנות חסר אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהם	
5	בניגוד לתקנות, המועצה לא הכינה תכנית בקרה שוטפת, הכוללת מה הנושאים שצריך לבדוק ומתי	יש להסדיר תכנית בקרה

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

6	תקנות הגדרת הפרטיות דורשות להכין מסמך הגדרות לכל מאגר מידע בנפרד שיכלול פרטים מסוימים לדוג': שם מנהל מאגר המידע, סוגי המידע השונים הכלולים במאגר, התמודדות עם סיכונים במקרה פגיעה באבטחת המידע ועוד.	יש להכין מסמך הגדרות
7	המועצה טרם החלה לנהל רשימת הרשאות תקפה לרבות רישום מעודכן של תפקידים, הרשאות גישה שניתנו להם.	יש להכין רשימת הרשאות

ה. דוח הביקורת המפורט בנושא הגנת הפרטיות- עמידה בתקנות

ה.1. מסמך הגדרות מאגר

תקנות 2017 - תקנה מספר 2 קובעת כי על בעל מאגר מידע להגדיר את המאגר במסמך הגדרות מאגר. להלן ציטוט מהתקנה:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

מסמך הגדרות המאגר

2. (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.



המועצה הכינה כנדרש בתקנות מסמך הגדרות מאגר לכלל המאגרים.

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות



במסמך הגדרות המאגר חסרה הדרישה של סעיף 6 פירוט הסיכונים העיקריים ואופן ההתמודדות איתם. מדובר בסעיף חשוב המכין את המועצה להתמודדות במקרה של התממשות אירוע של בטחון מידע.



תגובת מנמ"ר המועצה

"אכן חסר, מסמך מרכז לכלל המאגרים ו/או אירועי דלף מידע יוכן ויובא לאישור במהלך השבועיים הקרובים".

ה.2. רישום מאגרי מידע

סעיף 8 (א) לחוק קובע כי קיימת חובה לרשום את מאגרי המידע אצל הרשם. להלן לשון החוק:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ז) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

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 לעיין 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.

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**



המועצה רשמה את המאגרים כנדרש. יש לשים לב שלמאגר משאבי אנוש ומאגר ספקים טרם התקבל אישור ממשרד המשפטים.

ה.3. מינוי ממונה אבטחת מידע

על פי לסעיף 17 בחוק, ולפי תקנה מספר 3 בתקנות הגנת הפרטיות, המועצה מחויבת במינוי ממונה על אבטחת מידע. להלן הסעיף הרלוונטי בחוק:

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.

להלן הסעיף הרלוונטי מתוך התקנות:

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

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.



המועצה מינתה את מנמ"ר המועצה לכהן כממונה על אבטחת המידע. לדעתי המינוי עומד בניגוד לסעיף 3 (4) בתקנות (מסומן על ידי בקו תחתון) הדורש כי הממונה "לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו...".

כך גם עמדת הרשות להגנת הפרטיות. להלן ציטוט מתוך שאלות ותשובות שמופיעות באתר הרשות:

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

האם ממונה אבטחת מידע יכול שיהיה כפוף למנמ"ר (מנהל מערכות מידע)?

סעיף 3(4) לתקנות קובע כי הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי התקנות. המטרה של ההוראה היא לשמר את עצמאות שיקול דעתו וחוסר התלות של ממונה האבטחה. עמדת הרשות היא שלא ניתן להשיג מטרה זו אם ממונה האבטחה יכהן בעצמו גם כמנמ"ר של הארגון. חשש לניגוד עניינים קיים גם במקרה בו הממונה יהיה רק כפוף למנמ"ר, אולם ניתן לצמצם את החשש אם חוסר תלותו ועצמאות שיקול דעתו של הממונה תובטח בדרך יעילה אחרת. בשים לב למבנה הארגון ולמאפייניו הספציפיים, לדוגמא, באמצעות אפשרות דיווח ישיר למנכ"ל או לדירקטוריון, ומעורבות שלהם במינוי הממונה ובקביעת תנאי העסקתו.



מומלץ למנות את החברה החיצונית שנותנת שירותים למועצה כמיקור חוץ לממונה אבטחת מידע. כמובן שהמינוי כפוף להוראות החוק והתקנות הרלוונטיות.



תגובת מנמ"ר המועצה

"בכוונתנו לבחון אפשרות למנות מנהל אבט"מ CISO חיצוני מטעם חברת פריימסק שאיתה בוצע כל הליך האסדרה".

ה. נהלי אבטחת מידע

על פי תקנה מספר 4 משנת 2017, נדרש לקבוע נוהל אבטחה למאגר המידע. התקנות קובעות את הנושאים שצריכים להיכלל בנוהל אבטחת מאגרי המידע. סקרת את הנהלים הקיימים במועצה ולהלן תוצאות הבדיקה:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

מס'	תקנה	פירוט הדרישה	האם קיים במועצה
1	4 (ג) (1)	הוראות בעניין אבטחה פיזית וסביבתית של אתרי המאגר בהתאם לתקנה 6 (א) ו- (ב)	
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, אופן קביעת סיכונים אלה, ואופן הטיפול בהם	בוצע חלקית
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	
8	4 (ה)	בחינת הצורך בעדכון נוהל אבטחת מידע בתדירות של אחת לשנה לפחות	
9	4 (ד) (1)	אמצעי הזהיו והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9	
10 (*)	4 (ד) (2)	פירוט אופן הבקרה על השימוש במאגר המידע לרבות תיעוד הגישה למערכות המאגר, בהתאם לתקנה 1	
11	4 (ד) (3)	הוראות לעניין עריכת ביקורות תקופתיות לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16	
12 (*)	4 (ד) (4)	הוראות לעניין גיבוי הנתונים האמורים בתקנה 18 (א) (1)	

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

תגובת מנמ"ר המועצה (*)

סעיף 5- מנמ"ר המועצה צירף נוהל אבט"מ משתמשים והרשאות שמכיל את חלק מהנושאים.

תגובת המבקר: יש להכין נוהל הכולל את כול הנושאים המופיעים בתקנות

סעיף 7- בתגובת מנמ"ר המועצה לעניין נוהל התקנים ניידים נכתב כי "השימוש בהתקנים ניידים מוגבל למשתמשים מורשים בלבד".

תגובת המבקר: יש להכין נוהל מסודר ולא להסתפק באמירה כללית.

סעיף 10- תגובת המנמ"ר: "קיימת תוכנת תיעוד של גישה לרשת ולתיקיות הרשת".

תגובת המבקר: ההערה היתה בנוגע לתיעוד גישה למאגרי המידע ולא דווקא לרשת של המועצה.

סעיף 12- "יכתבו נהלי גיבוי התואמים את מערכות הגיבוי המצויות ברשותנו (גיבוי כפול, מקומי וענן)".

ה.5. תכנית לבקרה שוטפת

בהתאם לתקנה מס' 3 (3) הקובעת:

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

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס' 8)
הגנת הפרטיות- עמידה בתקנות**

משמעות התקנה כי על מנת לבצע בקורות באופן שיטתי שיכסו את כל נושאי הבקרה
קיימת חובה להכנת תכנית בקרה שוטפת.

נמצא כי למועצה טרם הוכנה תכנית לבקרה שוטפת 

תגובת מנמ"ר המועצה 

"יטופל מייד עם מינוי ממונה אבט"מ."

ה.6. מיפוי מערכות המאגר וביצוע סקר סיכונים
תקנה מספר 5 משנת 2017 קובעת שיש לבצע מיפוי מערכות המאגר. להלן התקנה:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

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 יישמחו 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 סיכונים 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 עמידות 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 בתקנת משנה (ג) ו-(ד) בסקר סיכונים או במבדקי חדירות, לפי העניין. אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה.



במועצה לא בוצע מיפוי של מערכות המאגר כנדרש בתקנות

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות



תגובת מנמ"ר המועצה

"בוצע סקר סיכונים מטעם חברת Allegronet I Cynomi בסוף שנת 2021, אשמח להעביר את תוצאותיו ככך שאדרש".

תגובת המבקר: קיבלתי את סקר הסיכונים והתרשמתי שמדובר בעבודה רצינית אך אין זה עונה על הצורך של מיפוי המערכות כפי שנדרש בסעיפי התקנה

ה.7. אבטחה פיזית וסביבתית

תקנה 6 מורה על אמצעי האבטחה הפיזיים שחלים על מאגרי המידע. להלן הוראות התקנה:

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 הביטחית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכניסה והוצאה של ציוד אל מערכות המאגר ומהן.



נמסר לביקורת כי חסר למועצה אמצעים לבקרה ולתיעוד של הכניסה והיציאה ושל הכנסת והוצאת ציוד מאתרי המאגר.

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**



תגובת מנמ"ר המועצה

הנוהל קיים ונמצא במסמך "נוהל אבטחה לשירותי רשת המחשוב ולמאגרי המידע"

תגובת המבקר: אכן קיים נוהל. אך ההערה הייתה שאין בקורות ותיעוד להכנסת והוצאות ציוד ואין גם התייחסות לכך בנהלים.

ה.8. ניהול הרשאות גישה וזיהוי ואימות

תקנות 8 ו-9 משנת 2017 מתייחסים לנושא הרשאות גישה וזיהוי ואימות. להלן ציטוט מהתקנות:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

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).

זיהוי ואימות

9. (א) בעל מאגר מידע ינקוט אמצעים מקובלים בנוסבות 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 הבינומית או הגבוהה –

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

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

(א) אופן הזיהוי; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחוק 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 הרשאה עשוי היה לדעת מיד עם סיום תפקידו של בעל הרשאה.

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**



המועצה טרם החלה לנהל רשימת הרשאות תקפה לרבות רישום מעודכן של תפקידים, הרשאות גישה שניתנו להם.



תגובת מנמ"ר המועצה

קיים נוהל המסדיר סוגיה זו, "נוהל אבטמ משתמשים והרשאות" רישום מדוייק יערך
ע"פ הנחיות ממונה האבט"מ לכשיופק לו כתב מינוי



המועצה מקפידה על קיום הרשאות גישה למאגרי המידע שלה וכן על זיהוי ואימות.

ה.9. חיבור התקנים

תקנה מספר 12 קובעת שיש להגביל או למנוע חיבור של התקנים ניידים. להלן התקנה:

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

התקנים בידי

12. בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים בידיים למערכות המאגר במתכונות ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנ"ד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה: בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ימקוט 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 הנ"ד.



בדיקתי העלתה כי אכן ישנה מגבלה של שימוש בהתקני USB חיצוניים ברשת

המועצה.

ה.10. בקרה ותיעוד גישה

תקנה מספר 10 משנת 2017 קובעת כי במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או גבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע. להלן ציטוט של התקנה:

**מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות**



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

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 ידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

למועצה חסר  מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע כנדרש בתקנות.

תגובת מנמ"ר המועצה

קיים מנגנון של בקרת גישה לכלל משאבי הרשת מוטמע בשרתי המועצה וזמין 24/7

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

תגובת המבקר: דגמתי מס' חודשים בגין חלק ממאגרי המידע על מנת לקבל את התיעוד האמור, והחברות החיצוניות שמנהלות את המאגר לא הצליחו לשלוח את הנתונים

ה.11. תיעוד של אירועי אבטחה

תקנה מספר 11 קובעת שנדרש לדווח על אירועי אבטחה. להלן ציטוט מהתקנה:

תיעוד של אירועי אבטחה

11. (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 הבינומית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכון של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יערך 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 שנעץ בראש הרשות הלאומית להגנת הסייבר. להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

**מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)
הגנת הפרטיות- עמידה בתקנות**

לדברי מנהל מערכות מידע, במועצה לא היו אירועי אבטחה

תגובת מנמ"ר המועצה

"אכן, לא נחשפנו, למעט ניסיון אחד (לפני כחודש וחצי) שנבלם בחומת האש הודות לחסימה שהוטמעה מראש. בעקבות הניסיון שלא צלח הוחמרה הגישה ונוסף מנגנון FA2 שהוטמע בחומת האש, וכן הסרה גורפת של כל המשתמשים והוספתם מחדש ע"פ צורך בלבד ולא באופן גורף/אוטומטי".

אין הדרכות על חשיבות דיווח אירועי אבטחה ולא קיימת מערכת ארגונית הדוחפת לדווח.

תגובת מנמ"ר המועצה

אכן, הנושא יטופל בשיתוף הממונה החדש.

המלצה

מומלץ שהמועצה תקדם את נושא החשיבות בדיווח ותעודד מנהלים ועובדים לדווח על אירועי אבטחת מידע.

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות

ו. סיכום

ביצעתי בדיקה של עמידה בתקנות הגנת הפרטיות. תוך כדי הבדיקה פרצה מלחמת חרבות ברזל ובעקבות כך היקף הבדיקה צומצם לבחינת העמידה בחלק מהתקנות בלבד. התרשמותי הכללית היא כי המועצה בהובלת מנכ"לית המועצה ומנמ"ר החלה בקידום ופיתוח נושא הגנת המידע ושכרה לשם כך שירותים של חברה חיצונית. בדיקתי העלתה כי חל שיפור משמעותי בנושא, יחד עם זאת עלו מס' הערות ודגשים שיש ליישם:

1. מינוי מנהל אבטחת מידע בלתי תלוי. ההמלצה היא למנות גורם חיצוני מקצועי.
2. בניית זיכרון ניהולי:
 - 2.1. הכנת תכנית בקרה שוטפת
 - 2.2. ניהול רשימת הרשאות תקפה לרבות רישום מעודכן של תפקידים, הרשאות גישה שניתנו להם.
 - 2.3. הכנת מסמך הגדרות לכל מאגר מידע (שיכלול פרטים מסוימים לדוג': שם מנהל מאגר המידע, סוגי המידע השונים הכלולים במאגר, התמודדות עם סיכונים במקרה פגיעה באבטחת המידע ועוד). ומיפוי מערכות המידע.
3. ניהול בקורות שוטפות:
 - 3.1. למועצה חסר מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המידע כנדרש בתקנות
 - 3.2. חסר בקורות על הכנסת והוצאת ציוד
 - 3.3. אין הדרכות על חשיבות דיווח אירועי אבטחה ולא קיימת מערכת ארגונית הדוחפת לדווח.

ז. תגובת ראש המועצה

תגובת ראש המועצה:

"המועצה תפעל על פי הממצאים לתקן את הליקויים על מנת לוודא אבטחת מידע של מאגרי המידע הקיימים והעתידים"

מסמך זה מכיל ממצאי ביקורת של מבקר המועצה. פרסומם בשלב זה
אסור עפ"י סעיף 145 ו. (ו) לצו המועצות המקומיות



מבקר המועצה וממונה על תלונות הציבור

מועצה אזורית רמת הנגב- דוח מבקר המועצה לשנת 2023 (דוח מס 8)

הגנת הפרטיות- עמידה בתקנות