דוח מבקר המדינה

ניהול מאגרי מידע במשרד הביטחון ואבטחתם

▪ כסלו התשפ"ו ▪ דצמבר 2025

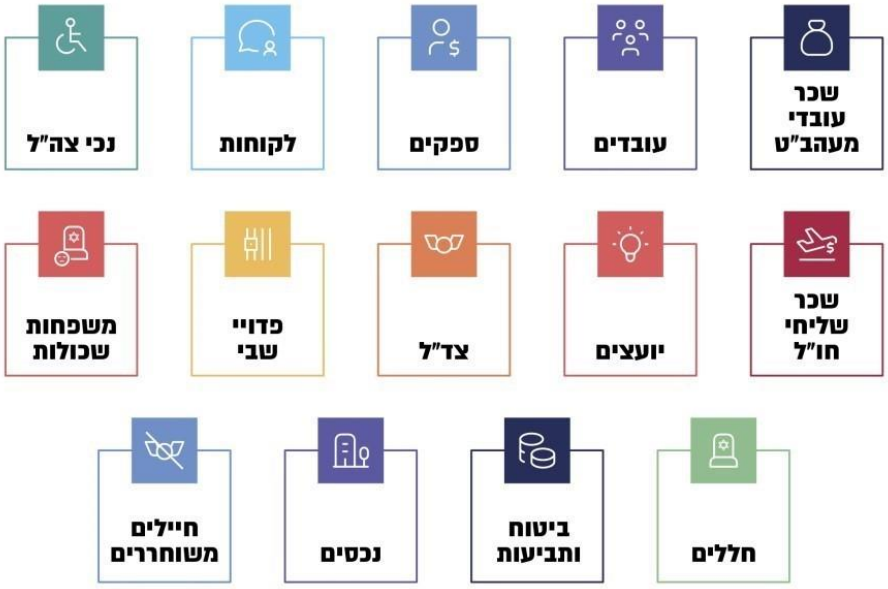
ניהול מאגרי מידע במשרד הביטחון ואבטחתם

מבוא

למשרד הביטחון תפקיד מרכזי במימוש יעדי הביטחון הלאומי של מדינת ישראל - הוא אמון בין היתר על הספקת האמצעים הנדרשים לבניין כוחו של צה"ל ולפעולתו, על הגנה על הנכסים של מערכת הביטחון, על טיפוח החוסן החברתי העוטף את השירות בצה"ל, ובכלל זה על מתן שירותים לציבור, ובהם טיפול במשפחות השכולות, שיקומם של נכי צה"ל וכוחות הביטחון וסיוע לחיילים משוחררים.

לצורך ביצוע משימותיו משתמש משרד הביטחון במאגרי מידע[1] רחבי היקף הכוללים מידע אישי, כגון נתונים על אישיותו של אדם, מעמדו האישי, מצבו הבריאותי, מצבו הכלכלי והכשרתו המקצועית. להלן מאגרי המידע שמשרד הביטחון רשם במרשם מאגרי המידע[2] שהוא בעל השליטה[3] בהם:

תרשים 1: **מאגרי המידע שמשרד הביטחון רשם במרשם מאגרי המידע שהוא בעל השליטה בהם**



על פי נתוני משרד הביטחון, בעיבוד משרד מבקר המדינה.

לפי התרשים משרד הביטחון רשם 14 מאגרי מידע, שהוא בעל השליטה בהם, במרשם מאגרי המידע שמנהלת הרשות להגנת הפרטיות שבמשרד המשפטים[4].

---

1 מאגר מידע הוא אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, למעט אוסף לשימוש אישי שאינו למטרות עסק או אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם (הגדרת "מאגר מידע" בסעיף 3 לחוק הגנת הפרטיות, התשמ"א-1981 (תיקון מס' 13 לחוק שייכנס לתוקף ב-14.8.25).

2 מרשם מאגרי המידע שמנהלת הרשות להגנת הפרטיות שבמשרד המשפטים, על פי חוק הגנת הפרטיות, התשמ"א-1981 (תיקון מס' 13 לחוק שייכנס לתוקף ב-14.8.25).

3 בעל שליטה במאגר הוא מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע, או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע (הגדרת "בעל שליטה" בסעיף 3 לחוק הגנת הפרטיות, התשמ"א-1981 (תיקון מס' 13 לחוק שייכנס לתוקף ב-14.8.25).

4 יצוין כי במרשם מאגרי המידע רשומים שני מאגרים נוספים (סך הכול 16) אולם לדברי משרד הביטחון הוא אינו בעל השליטה בהם.

איסוף מידע אישי, ניהולו במאגרי מידע ועיבודו במערכות ממוחשבות מאפשרים למשרד הביטחון לייעל את פעילותו ולשפר אותה. אולם, כמות המידע האגור במאגרי המידע הממוחשבים של משרד הביטחון והעובדה כי מדובר במידע דיגיטלי מגבירות את הסיכונים האפשריים לחשיפת מידע ולפגיעה בו, ובכלל זה:

1. **פגיעה בסודיות הנתונים (Confidentiality):** חשיפה או דליפה של מידע אישי מתוך מאגרי המידע בנוגע לפרטים שהם נושא המידע, ובפרט של מידע אישי במאגרים שיש בהם ערך ביטחוני.

2. **פגיעה באמינות (שלמות) הנתונים (Integrity):** שיבוש של המידע הקיים במאגרי המידע של משרד הביטחון באופן שהופך אותו לבלתי אמין כך שלא ניתן להשתמש בו לצורך ביצוע משימותיו של משרד הביטחון, העתקת המידע בלא הרשאה ועוד.

3. **פגיעה בזמינות הנתונים (Availability):** מחיקת המידע שבמאגרי המידע באופן שלא ניתן לאחזרם, השבתה של תשתיות התקשורת או של מערכות המידע, שהם שערי הכניסה למאגרים.

פגיעה בסודיות המידע, באמינותו ובזמינותו מגבירה את הסיכונים לפגיעה בפרטיותם של האנשים שמידע רגיש לגביהם שמור במאגרים אלו. הזכות לפרטיות היא אחת מזכויות האדם החשובות בישראל, והיא מעוגנת בחוק יסוד: כבוד האדם וחירותו, הקובע כי כל אדם זכאי לפרטיות ולצנעת חייו. חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק), ותקנותיו, ובהן תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, שהותקנו מכוח החוק (להלן - תקנות או תקנות אבטחת מידע), קובעים כללים והוראות בנוגע להגנה על פרטיות ולשמירה על מידע אישי במאגרי מידע.

על רקע ההתפתחויות הטכנולוגיות מרחיקות הלכת שהתרחשו מאז נחקק חוק הגנת הפרטיות, הגידול בהיקפם ובעוצמתם של האיומים על הפרטיות בעידן הדיגיטלי, האתגרים הייחודיים של אכיפת הגנת הפרטיות וההסדרים המודרניים של הגנה על מידע אישי במדינות מובילות בעולם, אישרה הכנסת באוגוסט 2024 את תיקון מס' 13 לחוק הגנת הפרטיות (להלן - תיקון 13 לחוק הגנת הפרטיות או תיקון 13 לחוק). תיקון זה ייכנס לתוקף באוגוסט 2025, והוא מעדכן באופן מקיף את חוק הגנת הפרטיות ומתאים אותו לאתגרים העכשוויים בהגנה על מידע אישי במאגרי מידע ממוחשבים. כמו כן, בינואר 2025 נכנסה לתוקפה הפעימה האחרונה לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. תקנות אלה הותקנו בעקבות תהליך בחינה מקיף שערכה נציבות האיחוד האירופי בנוגע לדיני הגנת הפרטיות בישראל, לצורך בחינת אשרור המעמד שניתן לישראל בשנת 2011 כמדינה שרמת הגנת הפרטיות שלה תואמת את תקן האיחוד האירופי[5]. תהליך הבחינה הושלם בינואר 2024 עם החלטת נציבות האיחוד האירופי לאשר מחדש את ההכרה במעמדה של ישראל כמדינה בעלת מעמד תאימות (Adequacy) בתחום הגנת הפרטיות. לפיכך, הן מחילות חובות נוספים על בעלי שליטה במאגרי מידע בישראל שמצוי בהם מידע שמקורו בין היתר במדינות החברות באיחוד האירופי.

הסיכונים להגנת הפרטיות ולאבטחת המידע שבמאגרי המידע גברו במהלך מלחמת חרבות ברזל נוכח התעצמות מתקפות הסייבר, שהן חלק בלתי נפרד מהמלחמה המודרנית, ובהן מתקפות על מאגרי מידע של גופים ציבוריים[6] והתגברות ניסיונות הודעות הדיוג (פישינג)[7] המכוונים לגורמים

---

[5] משנת 2018 נהוגה במדינות האיחוד האירופי רגולציה המכונה GDPR - (General Data Protection Regulation) להגנה על מידע.

[6] הרשות להגנת הפרטיות, דוח פעילות לשנת 2023, דצמבר 2024.

[7] הודעות דיוג (פישינג) הן אחת השיטות הנפוצות למתקפת סייבר, ומטרתן לגרום ליעד התקיפה לבצע פעולות מסוימות, כגון מסירת פרטים אישיים, הורדת תוכנה מזיקה או גניבת כסף או מידע, באמצעות שליחת הודעה.

בישראל, ובכלל זה לאנשי מערכת הביטחון לשעבר[8] - ניסיונות שהפכו מתוחכמים יותר וממוקדים יותר ביעד התקיפה באמצעות איסוף מידע מקדים בנוגע לתחומי העיסוק ולתחומי העניין של היעד[9]. בשנת 2024 חלה עלייה של 24% במספר אירועי הסייבר שאימת מערך הסייבר הלאומי בהשוואה לשנת 2023 (17,078 אירועי סייבר בשנת 2024 לעומת 13,040 בשנת 2023). המתקפות הנפוצות ביותר היו אירועי דיוג (פישינג) - בשנת 2024 אומתו 10,084 אירועים לעומת 3,301 בשנת 2023; 44% מאירועי הדיוג בשנת 2023 (1,449) אירעו משבעה באוקטובר ועד סוף שנת 2023. כמו כן, אומתו בשנת 2024 1,771 אירועי חדירה למערכות מחשוב לעומת 1,714 בשנת 2023, מחצית מאירועים אלה בשנת 2023 (873) אירעו משבעה באוקטובר ועד סוף שנת 2023[10].

ואכן, במהלך מלחמת חרבות ברזל התממש הסיכון לדלף מידע ממשרד הביטחון: באפריל 2024 פורסם בכלי התקשורת[11] כי באתר אינטרנט שהקימו פצחנים (האקרים) בין-לאומיים פורסם מידע שהודלף בידי גורמים עוינים מתוך פורטלים מינהליים של משרד הביטחון, ונכלל בהם מידע מזהה של עובדי המשרד, מידע על מכרזים ביטחוניים ועל מערכות טכנולוגיות של צה"ל, כגון פרטים על כלי רכב משוריינים, תשריטים הנדסיים ומידע טכני על מערכות צילום לווייניות[12].

לצד הסיכונים שמקורם בגורמים חיצוניים קיימים סיכונים להגנת הפרטיות ולאבטחת המידע שמקורם בגורמים פנימיים בארגון. דוגמה לכך היא התופעה של "שליפות מידע על ידי עובדים במגזר הציבורי"[13], שבה נעשה שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחֵר שלא למטרה שלשמה היא נמסרה. שליפות המידע גורמות לפגיעה קשה בפרטיות האזרחים שנמסר מידע לגביהם, והן מוגדרות כעבירה פלילית שעונשה עשוי להגיע לחמש שנות מאסר בפועל[14]. במשך השנים העמידה המדינה לדין פלילי ומשמעתי עובדי מדינה ממשרדי ממשלה ומרשויות שונות בגין עבירה זו[15].

הסיכון לדלף מידע ממשרד הביטחון כתוצאה מגורם פנימי התממש אף הוא. למשל, בשנת 2022 פורסם בכלי התקשורת[16] כי במסגרת רשימה של מקבלי דוחות תנועה בשנים 2016 - 2017 שאותה העביר משרד הביטחון לבקשת עמותה מסוימת במסגרת חוק חופש המידע, פורסמה בפומבי רשימה שכללה מספרי תעודות זהות, שמות ומספרי רכב של בכירים במשרד הביטחון. משרד הביטחון מסר לכלי התקשורת כי בעת העברת הרשימה נפלה טעות טכנית, ובמקום למחוק עמודות מטבלת האקסל שכללו שדות רגישים, העמודות הוסתרו כך שהתאפשר לבטל את ההסתרה ולראות את המידע הרגיש. משרד הביטחון אישר זאת למשרד מבקר המדינה בספטמבר 2024.

אל מול הסיכונים שפורטו לעיל נתקלת האכיפה על הגנת הפרטיות במאגרי מידע ממוחשבים באתגרים ייחודיים. להלן דוגמאות לאתגרים אלו, כפי שצוינו בדברי ההסבר לתיקון חוק הגנת הפרטיות[17].

---

8 מערך הסייבר הלאומי, "האיראנים מנסים לדוג אנשי מחקר בישראל", 31.10.24. https://www.gov.il/he/pages/iran_targeting_researchers_2024.

9 מערך הסייבר הלאומי, "הניסיונות האיראנים הפכו מתוחכמים יותר, ממוקדים יותר וממש תפורים ומותאמים לתחומי העניין של היעד", 24.11.24. https://www.gov.il/he/pages/24_11_2024.

10 לפי מערך הסייבר הלאומי, הדוח השנתי לסיכום שנת 2024, 17.2.25, בהתייחס לדיווחים מאזרחים ומארגונים שאומתו כאירועי סייבר.

11 למשל, **ישראל היום**, "האקרים הצליחו לחדור למערכות משרד הביטחון: חשש שמידע רגיש דלף" (9.4.24). https://www.israelhayom.co.il/tech/tech-news/article/15573329.

12 משרד הביטחון מסר לכלי התקשורת כי נפרץ אתר שאינו רגיש ואישר את התייחסותו זו למשרד מבקר המדינה בדצמבר 2024, לרבות מסירת התחקיר שבוצע בעקבות המקרה והפעולות שננקטו על ידו לטיפול בפרצת האבטחה.

13 הרשות להגנת הפרטיות, דוח פעילות לשנת 2023, דצמבר 2024.

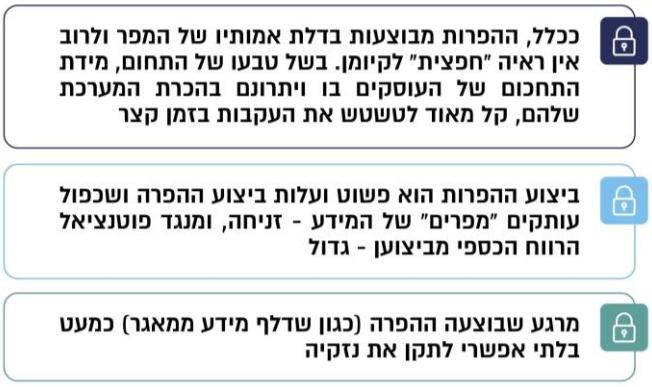
14 לפי סעיף 16 לחוק הגנת הפרטיות.

15 מתוך אתר האינטרנט של הרשות להגנת הפרטיות. https://www.gov.il/he/pages/privacy_videos_general

16 למשל, **דה מרקר**, "טעות קטנה באקסל חשפה ברשת פרטים של בכירים במשרד הביטחון" (24.8.22), https://www.themarker.com/captain-internet/2022-08-24/ty-article/.premium/00000182-cf9f-d1de-a7c3-dfdf3bca0000.

17 לפי דברי ההסבר לתיקון חוק הגנת הפרטיות, עמ' 420.

תרשים 2 : **דוגמאות לאתגרים הייחודיים באכיפה על הגנת הפרטיות במאגרי מידע ממוחשבים**



התממשות הסיכונים להגנת הפרטיות ולאבטחת המידע שבמאגרי המידע של משרד הביטחון עלולה להיות בעלת השלכות רוחביות - על הפרט, שמידע לגביו שמור במאגרים, על תפקודו ופעילותו של משרד הביטחון, ועל ביטחון המדינה, כמתואר בתרשים שלהלן.

תרשים 3 : **השלכות אפשריות כתוצאה מהתממשות הסיכונים למידע שבמאגרי המידע**

התממשות הסיכונים למאגרי המידע של משרד הביטחון עלולה לגרום למשל לחשיפה של מידע אישי על חיילים שנפצעו במלחמה (מאגר נכי צה"ל) - מידע שהוא בעל ערך בין היתר לגורמים המעוניינים להציע להם שירותים שונים כגון ליווי משפטי, או מידע אישי על חטופים מטבח שבעה באוקטובר ששוחררו מעזה (מאגר פדויי שבי) והפכו, בעל כורחם, לעניין ציבורי. חשיפת מידע זה עלולה לגרום לאיבוד שליטה על השימוש במידע עליהם, לגרום להם להפסד כספי, לפגיעה בסודיות ועוד.

נוסף על כך, חשיפת מידע או שיבוש מידע ממאגרים שיש בהם ערך ביטחוני, דוגמת מאגר עובדי משרד הביטחון ומאגר ספקי המשרד, שנדרש לשמור על חסיונם, עלולים לפגוע ברציפות התפקודית של משרד הביטחון וביכולתו לממש את יעדי הביטחון הלאומי של מדינת ישראל שבאחריותו, בדגש על יכולתו לספק את האמצעים הנדרשים לבניין כוחו של צה"ל ולפעולתו, לגרום לו נזק תדמיתי, לפגוע ביחסיו עם ספקים ולקוחות ולחשוף אותו לתביעות ולקנסות כספיים. כמו כן חשיפת מידע או שיבוש מידע ממאגרים שיש בהם ערך ביטחוני עלולים לפגוע בפעילותם של גופים ביטחוניים נוספים.

יתרה מכך, לעניין זה השפעה תודעתית - הדבר עלול אף לזרוע בהלה ותחושת חוסר ביטחון בציבור, לפגוע בקשרי החוץ של המדינה בהקשרים ביטחוניים-מדיניים ולפגוע במערכותיה החיוניות של מדינת ישראל.

פעולות הביקורת

בחודשים אוגוסט 2024 עד ינואר 2025 בדק משרד מבקר המדינה את האופן שבו משרד הביטחון מנהל את מאגרי המידע שהוא בעל השליטה בהם ואת האופן שבו הוא מאבטח אותם בראי הדרישות החלות עליו כפי שנקבעו בחוק הגנת הפרטיות ובתקנות. יצוין כי הביקורת לא עסקה באבטחת מידע בהיבטי סייבר. הביקורת נעשתה במשרד הביטחון - באגף תקשוב וניהול מערכות מידע (להלן - אגף התקשוב) ובאגף ביטחון ; במשרד המשפטים - ברשות להגנת הפרטיות. בדיקות השלמה נעשו באגף שיקום נכים שבמשרד הביטחון.

יצוין כי מכיוון שתיקון 13 לחוק הגנת הפרטיות אושר בכנסת באוגוסט 2024, והוא ייכנס לתוקף באוגוסט 2025, לאחר מועד סיום הביקורת, נבדקה פעילותו של משרד הביטחון אל מול הוראות החוק טרם התיקון ובהלימה לדרישות שיחולו עליו בראייה צופה פני עתיד. בהתאם, ההגדרות והמונחים וכן ההמלצות המוצגים בדוח זה בהתייחס לחוק ולתקנות הם בהתאם לתיקון 13 לחוק.

בקרת משרד הביטחון על יישום תקנות אבטחת מידע במאגרי המידע וניהול המאגרים

בגוף ציבורי שבבעלותו או בהחזקתו מאגר מידע, מנהל המאגר הוא המנכ"ל או מי שהמנכ"ל הסמיכו לכך[18]. מנכ"ל משרד הביטחון מינה את סמנכ"ל וראש אגף התקשוב (להלן - ראש אגף התקשוב) לנהל את מאגרי המידע הקיימים באגפי משרד הביטחון ויחידותיו בהתאם לחוק הגנת הפרטיות והתקנות, לרבות ניהול רישום מדויק של המאגרים הקיימים במשרד הביטחון, קביעת סדרי הניהול שלהם, הגדרת האמצעים הטכנולוגיים לאבטחת המידע האגור בהם, קיום מכלול הדרישות לאבטחת המידע ועוד[19].

יודגש כי על פי תקנות אבטחת מידע, החובות החלות בתקנות על בעל השליטה במאגר מידע חלות גם על מנהל המאגר[20]. לפיכך, ראש אגף התקשוב במשרד הביטחון נושא באחריות לעמידה בחובות המנויות בתקנות בנוגע למאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם.

אגף התקשוב אמון על פיתוח מערכות ממוחשבות, תפעולן ותחזוקתן עבור כלל האגפים והיחידות של משרד הביטחון, על הפעלת מערכות תקשורת וניהול מרכזי המחשבים, על ניהול מסדי הנתונים של משרד הביטחון ותקינותם ועוד. לגורמים שונים באגף התקשוב יש ממשקי עבודה עם תחום מאגרי המידע, כמפורט בתרשים שלהלן.

---

18 הגדרת "מנהל מאגר" בסעיף 3 לחוק הגנת הפרטיות (תיקון 13 לחוק).

19 לפי הוראת משרד הביטחון מס' 70.21 בנושא חוק הגנת הפרטיות - ניהול ואבטחה של מידע ומאגרי מידע במשרד הביטחון מאוגוסט 2020.

20 לפי תקנה 19(א) לתקנות.

תרשים 4: **גורמים מרכזיים באגף התקשוב שלהם יש ממשקי עבודה עם מאגרי המידע**

הממונה על אבטחת מידע במאגרי המידע של משרד הביטחון

בפגישה שקיימו נציגי משרד מבקר המדינה בספטמבר 2024 עם ראש היחידה למסדי נתונים באגף התקשוב היא מסרה כי נוסף על תפקידה זה היא מוגדרת כממונה על אבטחת המידע במאגרי המידע של משרד הביטחון, אך היא אינה ממלאת תפקיד זה בפועל. עוד היא מסרה כי אין בעל תפקיד באגף שאחראי לזהות את הדרישות החלות על משרד הביטחון מתוקף חוק הגנת הפרטיות והתקנות, ובכלל זה לתקף את העמידה בהן ולבצע בקרה על כך, ולא ידוע לה על קיומה של תוכנית לבקרה שוטפת על העמידה בדרישות או על ביצוע בקרות תקופתיות.

לבקשת משרד מבקר המדינה לקבל את כתב המינוי של ראש היחידה למסדי נתונים לתפקיד הממונה על אבטחת המידע במאגרי המידע של משרד הביטחון, העביר אגף התקשוב כתב מינוי שבו מצוין כי ראש אגף התקשוב ממנה את ראש היחידה למערכות מחשוב ליתרון הגנתי בסייבר לממונה על אבטחת המידע והגנת הפרטיות במשרד הביטחון החל באוקטובר 2024 (לאחר מועד תחילת ביקורת זו). בכתב המינוי פורטו תפקידי הממונה, ובכלל זה להסדיר את תהליכי ניהול המידע הדיגיטלי במערכות המידע שבמשרד הביטחון, לבצע בקרה שוטפת על תוכנית העבודה השנתית בנושא הגנת הפרטיות בהתאם לתקנות אבטחת מידע, לשמש סמכות מקצועית ומוקד ידע בנושא אבטחת מידע והגנת הפרטיות, לשמש איש קשר מול הרשות להגנת הפרטיות ועוד.

בפגישה שקיימו נציגי משרד מבקר המדינה בנובמבר 2024 עם הממונה החדשה על אבטחת מידע במאגרי המידע, היא מסרה כי תפקיד זה מתווסף למשימותיה כראש היחידה למערכות מחשוב ליתרון הגנתי בסייבר, וכי לצורך מימוש תפקיד זה בכוונתה להשתתף בהכשרה בנושא הגנת הפרטיות על מאגרי מידע. כמו כן, בכוונת אגף התקשוב לשכור את שירותיה של חברה שתייעץ לאגף בנושא הגנת הפרטיות ותבצע את הפעולות הנדרשות מהממונה על אבטחת מידע וממנהל מאגרי המידע בהתאם לחוק ולתקנות, לרבות מיפוי מאגרי המידע שבבעלות משרד הביטחון, הכנת תוכנית לבקרה שוטפת וביצועה, ביצוע מבדקי חדירה וסקרי סיכונים ועוד. התקציב עבור שירותי הייעוץ יוקצה לה במסגרת תוכנית העבודה לשנת 2025.

יצוין כי לפי תיקון 13 לחוק הגנת הפרטיות שייכנס לתוקף באוגוסט 2025, העומדים בראש גופים ביטחוניים, ובכלל זה משרד הביטחון על יחידות הסמך שלו והממונה על הביטחון במערכת הביטחון, ימנו מפקח פרטיות; זאת בהתייעצות עם ראש הרשות להגנת הפרטיות ובהתאם לתנאי הכשירות וההכשרה שיורה עליהם ראש הרשות. מפקח הפרטיות בגוף הביטחוני יהיה כפוף ישירות לראש הגוף הביטחוני או למי מטעמו ויונחה מקצועית על ידי הרשות להגנת הפרטיות. הוא יפקח על יישום הוראות חוק הגנת הפרטיות בגוף הביטחוני, יקיים בקרה על ביצוען, ובכלל זה יכין

תוכנית עבודה שנתית לפיקוח על הוראות החוק ולבדיקת הפרות של הוראות שראש הרשות מוסמך להורות על הפסקת הפרתן. תוכנית זו, תאושר על ידי ראש הגוף הביטחוני וראש הרשות, ומפקח הפרטיות יגיש לראש הגוף הביטחוני ולראש הרשות דין וחשבון שנתי על אופן ביצוע התוכנית ועל קיום הוראות הדין בתחום הפרטיות בגוף הביטחוני[21].

הסדר מיוחד זה לעניין הגופים הביטחוניים נועד לתת מענה לחשיבות המיוחדת לפיקוח ולאכיפה של הוראות החוק הנוגעות למאגרי מידע בגופים ביטחוניים אשר כחלק מפעילותם ולצורך מילוי תפקידם אוספים באופן שיטתי מידע רב על אנשים, אולם חלק ניכר מפעילותם בנוגע למאגרי מידע היא מסווגת, וחשיפה של גורם חיצוני למידע עלולה להביא לפגיעה בביטחון המדינה[22].

בביקורת עלה כי בניגוד לנדרש בחוק הגנת הפרטיות ובתקנות, שלפיהם ימונה ממונה אבטחת מידע במאגרי המידע שיבצע בקרה שוטפת על העמידה בדרישות שבתקנות אבטחת מידע, אין בעל תפקיד במשרד הביטחון שאחראי לזהות את הדרישות החלות על המשרד מתוקף החוק והתקנות, ובכלל זה לתקף את העמידה בהם ולבצע בקרה על כך. עוד עלה כי עד אוקטובר 2024 ראש אגף התקשוב במשרד הביטחון, המופקד על ניהול מאגרי המידע ונושא על פי חוק באחריות ישירה לאבטחת המידע שבמאגרי המידע במשרד הביטחון ולעמידה בחובות המנויות בתקנות בנוגע למאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם, לא וידא שהממונה על אבטחת המידע במאגרי המידע ממלאת את תפקידיה בהתאם לנדרש בתקנות; וממילא הוא לא ביצע בקרה על עמידתו של משרד הביטחון בדרישות החלות על המשרד מתוקף התקנות, חרף חשיבותן של תקנות אלו להגנה על פרטיותם של אנשים שמידע רגיש לגביהם שמור במאגרים וחרף הסיכונים הרבים הנשקפים למאגרים והשלכותיהם הרוחביות - בהיבטי הפרט, הארגון וביטחון המדינה.

יצוין כי באוקטובר 2024, בעקבות ביקורת זו, מינה ראש אגף התקשוב ממונה חדשה על אבטחת המידע במאגרי המידע והקנה לה סמכויות בנושא. תפקידה זה מתווסף למגוון משימותיה כראש היחידה למערכות מחשוב ליתרון הגנתי בסייבר באגף התקשוב.

על ראש אגף התקשוב, המופקד על ניהול מאגרי המידע במשרד הביטחון, לוודא כי ביכולתה של הממונה על אבטחת המידע במאגרי המידע לבצע את תפקידה כנדרש, כי היא תקבל את ההכשרה הנדרשת, וכי יוקצו לנושא המשאבים הדרושים.

על הממונה על אבטחת המידע במאגרי המידע שבמשרד הביטחון לממש את תפקידה כנדרש בתקנות ובכלל זה להכין תוכנית לבקרה שוטפת על העמידה בדרישות שבתקנות, לבצע את הבקרה ולהביא את ממצאיה לידיעתם של כלל הגורמים הנוגעים בדבר.

על מנכ"ל משרד הביטחון למנות מפקח פרטיות כמתחייב בתיקון 13 לחוק הגנת הפרטיות שייכנס לתוקף באוגוסט 2025, לוודא כי קיימת חלוקת תפקידים ברורה בין הממונה על אבטחת המידע במאגרי המידע ובין מפקח הפרטיות שימונה במשרד הביטחון, ולעקוב אחר ביצוע תפקידם.

בתגובתו על ממצאי הביקורת ממאי 2025 ציין משרד הביטחון כי הוא אכן מינה ממונה על אבטחת מידע במאגרי המידע שבמשרד וכן התקשר עם חברת ייעוץ ליישום דרישות חוק הגנת הפרטיות

---

21 לפי סעיפים 23יט' עד 23כד' לתיקון 13 לחוק (סימן ה': פיקוח ובירור מינהלי בגופים ציבוריים לפי חוק להסדרת הביטחון בגופים ציבוריים). נוסף על התפקידים שצוינו לעיל, מפקח הפרטיות בגוף ביטחוני יבדוק את נוהלי הגוף הביטחוני ומדיניותו בתחום הגנת הפרטיות ועמידתם בהוראות הדין; ידווח מיידית לראש הרשות להגנת הפרטיות על ממצאים של פעולות הפיקוח והבדיקה שביצע, זאת בכפוף להוראות המידור החלות על הגוף הביטחוני; יבצע בקרה על אופן תיקון הליקויים שהתגלו בממצאי הפיקוח והבדיקה; ויכשיר וידריך את עובדי הגוף הביטחוני בנושאי פרטיות.

22 לפי דברי ההסבר לתיקון חוק הגנת הפרטיות, עמ' 441.

ותקנות אבטחת מידע. עוד ציין משרד הביטחון כי הוא התניע תהליך למינוי מפקח פרטיות במשרד בהתאם לנדרש בתיקון 13 לחוק הגנת הפרטיות.

המיפוי והרישום של מאגרי המידע

גוף ציבורי חייב לרשום את מאגרי המידע שהוא בעל השליטה בהם במרשם מאגרי המידע שמנוהל בידי ראש הרשות להגנת הפרטיות שבמשרד המשפטים[23], ועליו להודיע לראש הרשות על שינויים מסוימים הנוגעים למאגרים, דוגמת שינוי בסוגי המידע הכלולים במאגר, שינוי במטרות השימוש במידע ועוד[24].

יודגש כי דיני הגנת הפרטיות ותקנות אבטחת מידע חלים על כל מאגר מידע אישי, אם המאגר נרשם במרשם המאגרים ואם לאו. מכאן שהגוף הציבורי נדרש למפות את כלל המידע שברשותו כדי לדעת אם הוא כולל מידע אישי כהגדרתו בחוק ובתקנות ואם חלות עליו דרישות מתוקף החוק והתקנות, לרבות החובה לרשום את המידע כמאגר מידע במרשם המאגרים. לדוגמה, חלק ניכר מההקלטות המתבצעות באמצעות מצלמות מעקב עונות להגדרת מאגר מידע בהתייחס למידע מזוהה או למידע שניתן לזיהוי על אודות אדם מסוים, ולכן גוף ציבורי נדרש לבחון גם את ההקלטות ממצלמות המעקב שברשותו[25].

כאמור, נוסף על חוק הגנת הפרטיות ותקנות אבטחת מידע, בינואר 2025 נכנסה לתוקפה הפעימה האחרונה לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. מתוקף תקנות אלו, בעלי שליטה במאגרי מידע בישראל שמחזיקים למשל במידע שהועבר להם ושמצוי במאגרים שלהם בנוגע לאזרחי האיחוד האירופי, נדרשים לנקוט אמצעים נוספים לגבי כלל המידע האגור במאגרי מידע אלה (לרבות מידע בנוגע לאזרחים ישראלים), דוגמת מחיקה של מידע ויידוע של נושאי המידע[26]. מכאן שגופים ציבוריים נדרשים למפות את המידע שברשותם גם בהתאם לתקנות אלו ולסייגים שנקבעו בהן.

בהתאם לחוק הגנת הפרטיות רשם משרד הביטחון במרשם מאגרי המידע 14 מאגרי מידע שבבעלותו, ומשנת 2007 אגף התקשוב לא העביר למשרד המשפטים עדכונים נוספים בנוגע למאגרים. לשאלת משרד מבקר המדינה, באוקטובר 2024 מסר אגף התקשוב כי לא קיימים במשרד הביטחון מאגרי מידע נוספים על אלו שרשומים במשרד המשפטים. בדצמבר 2024, בעקבות ביקורת זו, הנחה ראש אגף התקשוב את כלל ראשי האגפים וראשי היחידות במשרד הביטחון לבצע מיפוי מלא של מאגרי המידע שקיימים באגפיהם וביחידותיהם אשר מועברים ממשרד הביטחון לגורמים חיצוניים או מתקבלים מהם.

בביקורת עלה כי שלא בהתאם לנדרש בחוק הגנת הפרטיות כי בעל שליטה במאגר מידע ירשום את המאגרים במרשם מאגרי המידע ויודיע על שינויים מסוימים הנוגעים למאגרים, אגף התקשוב לא מיפה את כלל המידע שבבעלות משרד הביטחון משנת 2007 כדי לדעת אם הוא כולל מידע אישי כהגדרתו בחוק ובתקנות, ואם חלות על משרד הביטחון דרישות נוספות מתוקף החוק, לרבות החובה לרשום מידע זה במרשם המאגרים. בעקבות הביקורת, בדצמבר 2024 הנחה ראש אגף התקשוב את ראשי האגפים והיחידות במשרד הביטחון לבצע מיפוי של מאגרי המידע באגפיהם וביחידותיהם. עם זאת, הנחייתו נגעה רק למידע שהועבר ממשרד הביטחון לגורמים מחוץ למשרד או התקבל מהם. נכון למועד סיום הביקורת, ינואר 2025, טרם הסתיים המיפוי.

---

23 לפי סעיף 8(ג)4 לחוק. יצוין כי לפי תיקון 13 לחוק, גוף ציבורי אינו חייב לרשום מאגר מידע הכולל מידע אישי על עובדי הגוף הציבורי בלבד (כגון מאגר נתוני עובדים).

24 לפי סעיף 9(ד) לחוק.

25 לפי הנחיית הרשות להגנת הפרטיות 4/2012 בנושא שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן.

26 בשים לב לסייגים המנויים בתקנות, כגון מידע שהעביר אדם על עצמו, שימוש במידע הנדרש למטרת הגנה על ביטחון המדינה בהיקף הנחוץ והמידתי למטרה זו ועוד.

במצב זה משרד הביטחון לא הכיר בכך שייתכן שיש בבעלותו מאגרי מידע נוספים שלגביהם הוא נדרש לפעול בהתאם להוראות שבחוק הגנת הפרטיות ובתקנות, ובכלל זה מאגרים שכוללים מידע אישי רגיש דוגמת מידע על צנעת חיי המשפחה של אדם; מצב בריאותו; עברו הפלילי; נתוני שכרו; אמונותיו הדתיות; מוצאו; הערכת מאפייני אישיותו המהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה; נתוני מיקומו ונתוני תעבורה[27]. מידע אישי רגיש מסוג זה עשוי להיכלל למשל במאגרי המידע של מבדקי התאמה מהימנותיים וביטחוניים שמבצע משרד הביטחון לכלל האוכלוסיות שמועסקות בו ובמאגרי המידע של מבדקי הערכה לגיוס עובדים.

לפיכך משרד הביטחון אינו מודע לכך שייתכן שחלות עליו חובות נוספות בנוגע למידע אישי שהוא בעל השליטה בו וכן חובות מתוקף תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023, שעמידה בהן מקלה על קיום קשרי מסחר עם המדינות החברות באיחוד האירופי, והיעדרה עלול לפגוע בקשרי החוץ עם מערכות ביטחון זרות שלהן חשיבות רבה למימוש יעדי הביטחון הלאומי של מדינת ישראל.

על ראש אגף התקשוב להנחות את ראשי האגפים וראשי היחידות במשרד הביטחון לבצע מיפוי מלא של כלל המידע האישי שקיים אצלם, ולא רק בנוגע למידע שמועבר ממשרד הביטחון לגורמים מחוץ למשרד או מתקבל מהם. כמו כן, עליו לוודא כי המיפוי יתייחס גם לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. לאחר מכן, על ראש אגף התקשוב לזהות את הדרישות החלות על משרד הביטחון בהתאם לממצאי המיפוי, לרבות החובה לרשום אותם במרשם המאגרים.

כמו כן, על אגף התקשוב לבצע מיפוי תקופתי בנוגע למאגרי המידע שבמשרד הביטחון - אלו הקיימים ואלו שיתווספו במעלה הדרך, דבר שיסייע לו להפנים את החובות המוטלות עליו ולהגביר את הציות לחוק הגנת הפרטיות ולתקנות. עוד מומלץ כי אגף התקשוב יעגן בנוהל את מחזורי הזמן של המיפוי.

מסמך הגדרות מאגר וסיווג המאגרים

בעל שליטה במאגר מידע נדרש להכין מסמך הגדרות מאגר שמתאר היבטים מרכזיים שנוגעים למאגר[28]. על מסמך זה לכלול בין השאר את הנושאים האלה:

תרשים 5: **נושאים עיקריים שיש לכלול במסמך הגדרות מאגר**

לפי תקנות אבטחת מידע, בעיבוד משרד מבקר המדינה.

27 דוגמאות למידע אישי רגיש כפי שפורטו בתיקון 13 לחוק.

28 לפי תקנה 2(א) לתקנות.

כמו כן, בעל שליטה במאגר מידע נדרש לעדכן את המסמך בכל עת שנעשה שינוי משמעותי בנושאים המפורטים לעיל ולבחון את הצורך בעדכון כאמור בשל שינויים טכנולוגיים וארגוניים או בשל אירועי אבטחה[29] בכל שנה עד 31 בדצמבר.

נוסף על הכנת מסמך הגדרות מאגר, נדרש בעל השליטה במאגר לסווג את המאגר בהתאם לסיכוני האבטחה שהוא מייצר באחת משלוש רמות אבטחה - בסיסית, בינונית או גבוהה. על כלל מאגרי המידע של גופים ציבוריים חלה רמת אבטחה בינונית ומעלה, וכל מאגר שיש בו מידע על אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה בו גדול מ-100 הוא בעל רמת אבטחה גבוהה (הדרישות שבתקנות משתנות בהתאם לרמת האבטחה)[30]. מכאן שמאגרי המידע שבבעלות משרד הביטחון נדרשים להיות מסווגים ברמת אבטחה בינונית או גבוהה.

הכנת מסמך הגדרות מאגר מספקת לבעל השליטה במאגר המידע תשתית לסיווג רמת האבטחה של כל מאגר, וכפועל יוצא מכך מאפשרת לו לדעת אילו מהדרישות בתקנות חלות עליו[31].

בפגישה שקיימו נציגי משרד מבקר המדינה בספטמבר 2024 עם הממונה על אבטחת המידע במאגרי המידע דאז (ראש היחידה למסדי נתונים) היא ציינה כי לא ידוע לה אם קיים באגף התקשוב מסמך הגדרות מרכז למאגרי המידע שבבעלות משרד הביטחון. עוד היא ציינה כי באגף התקשוב לא ידוע מהן רמות האבטחה החלות על מאגרי המידע של משרד הביטחון ומי מסווג אותם.

לבקשת משרד מבקר המדינה הכין אגף התקשוב מסמך המרכז את רשימת 14 המאגרים הרשומים במרשם המאגרים ובו תיאור קצר בנוגע לסוגי המידע הקיימים בכל מאגר, מספר הפרטים הרשומים בו, מספר בעלי ההרשאה אליו, עצם קיומו של מסמך הגדרות מאגר ועוד. מהמסמך עלה כי ל-11 מאגרים מתוך ה-14 שרשומים במרשם המאגרים (78% מהמאגרים הרשומים) קיים מסמך הגדרות מאגר, ול-3 לא קיים מסמך זה. אולם, בפגישות שקיימו נציגי משרד מבקר המדינה בספטמבר ובאוקטובר 2024 עם נציגי היחידות לפיתוח היישומים המקושרים למאגרי מידע שונים עלו הדברים האלה: (א) בנוגע למאגרים נכי צה"ל, משפחות שכולות וחללים, אשר לגביהם צוין במסמך המרכז כי קיים מסמך הגדרות מאגר - לא קיים מסמך הגדרות מאגר; (ב) בנוגע למאגרים עובדים ויועצים אשר גם לגביהם צוין כי קיים מסמך הגדרות מאגר, הוכן מסמך מעין זה באפיון הראשוני להקמת מערכת המידע המקושרת למאגרים אלו אך לא ידוע על קיומו של מסמך עדכני.

משרד מבקר המדינה סיווג את המאגרים בהתאם למאפיינים שלהם על בסיס המסמך המרכז ומצא כי 8 מתוך 14 המאגרים שרשומים במרשם המאגרים (57%) הם ברמת אבטחה גבוהה, והיתר (6 מאגרים, שהם 43% מהמאגרים הרשומים) הם ברמת אבטחה בינונית, כמפורט בתרשים שלהלן.

---

29 תקנות 2(ב) ו-11 בהתאמה.

30 התוספת הראשונה והתוספת השנייה לתקנות.

31 הרשות להגנת הפרטיות, **מסמך הגדרות מאגר**, אתר האינטרנט של הרשות.

תרשים 6: **מאגרי המידע שמשרד הביטחון רשם במרשם המאגרים, לפי רמת האבטחה שלהם**

על פי נתוני משרד הביטחון, בעיבוד משרד מבקר המדינה.

בביקורת עלה כי בניגוד לנדרש בתקנות אבטחת מידע, שלפיהן יוכן מסמך הגדרות מאגר שמתאר היבטים מרכזיים שנוגעים לו וכי המאגר יסווג בהתאם לסיכוני האבטחה שהוא מייצר, אגף התקשוב במשרד הביטחון לא הכין מסמך כאמור לכל אחד ממאגרי המידע שהוא בעל השליטה בהם, והוא לא סיווג את המאגרים בהתאם לרמות האבטחה החלות עליהם (בינונית או גבוהה). במצב זה אין לאגף התקשוב תמונת מצב מלאה ועדכנית בנוגע לכל המאגרים שהוא מנהל, אשר תאפשר לו להתאים את מענה ההגנה הנדרש עבורם בהתאם לסיכונים שהם מייצרים.

יתרה מכך, מאוגוסט 2025, עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, עלול משרד הביטחון להיות חשוף לעיצומים כספיים בסכום שבין 20,000 ש"ח ל-320,000 ש"ח בגין הפרות שונות של תקנות אבטחת מידע בנוגע לכל מאגר; סכום העיצומים גדל ככל שעולה רמת האבטחה שחלה על המאגר. בהינתן שלפי בדיקת משרד מבקר המדינה 8 מתוך 14 המאגרים שמשרד הביטחון רשם במרשם המאגרים (57%), הם ברמת אבטחה גבוהה, הוא חשוף במידה רבה לעיצומים בסכום הגבוה ביותר.

על אגף התקשוב להכין מסמך הגדרות מאגר לכל מאגר מידע שמשרד הביטחון הוא בעל השליטה בו כנדרש בתקנות ולבחון את הצורך בעדכון המסמך בשל שינויים טכנולוגיים וארגוניים או בשל אירועי אבטחה, זאת בכל שנה עד 31 בדצמבר. כמו כן, על אגף התקשוב לסווג את רמת האבטחה שחלה על כל מאגר בשים לב לדגשים בתיקון 13 לחוק לעניין הקריטריונים לסיווג.

מידע עודף במאגרי מידע

לפי חוק הגנת הפרטיות, שימוש במידע שבמאגר מידע מותר רק למטרה שלשמה הוקם המאגר[32]. בתקנות אבטחת מידע נקבע כי על בעל השליטה במאגר מידע לוודא אחת לשנה שהמידע השמור במאגר אינו רב מן הנדרש בהתאם למטרות המאגר[33].

מידע שנשמר במאגר מידע, אשר אינו רלוונטי או אינו נדרש להשגת המטרה שלשמה הוא נאסף או להשגת מטרות המאגר שבו הוא נשמר, נחשב מידע עודף. מידע עודף יכול להיווצר כבר בשלב איסוף המידע הראשוני או להפוך לכזה במהלך שמירתו לאורך זמן במאגרי המידע[34].

בפגישות שקיימו נציגי משרד מבקר המדינה בספטמבר ובאוקטובר 2024 עם נציגי היחידות לפיתוח היישומים המקושרים למאגרי מידע שונים[35] נמסר כי אגף התקשוב אינו בוחן אם קיים מידע עודף במאגרים כיוון שההחלטה מהו מידע עודף היא בהתאם לשיקול דעתו של כל מנהל אגף במשרד הביטחון שמשתמש במאגרי המידע ויודע מהם הצרכים שלשמם נדרש המידע. עוד נמסר כי קיים צורך לשמור מידע היסטורי במאגרי המידע, למשל במצב שבו אדם פנה למשרד הביטחון בבקשה כלשהי ונדחה אך החליט להגיש ערעור כעבור כמה שנים ולכן נדרש מידע קודם בענייננו. כמו כן, נמסר כי אגף התקשוב לא קיבל בקשות מגורמים רלוונטיים באגפי המשרד להסיר מידע עודף, ולא ידוע על קיומה של בדיקה סדורה ושיטתית של מידע עודף במאגרים.

עם זאת, במקרה מסוים הושמטו נתונים ממאגר מידע שמשרד הביטחון הוא בעל השליטה בו - מאגר נכי צה"ל, המשמש את אגף שיקום נכים בעבודתו. מאגר נכי צה"ל מכיל נתונים מקום המדינה הכוללים מידע משלב הבקשה להכרה בנכה ועד השלב שבו מקבל הנכה תגמולים באופן שוטף. ניהול הנתונים שבמאגר מתבצע באמצעות מערכת מידע בשם שֶׁמֶש. במרץ 2024 העביר אגף התקשוב את מערכת שמש, ובכלל זה את מאגר נכי צה"ל המקושר אליה, מרשת תקשורת מסווגת לרשת תקשורת שאינה מסווגת (בלמ"סית) כדי להנגיש את המידע ולשפר את השירות לאוכלוסיות הזכאים[36]. בעת המעבר הנחה אגף ביטחון שבמשרד הביטחון את אגף התקשוב להשמיט נתונים מסוימים מתוך המאגר שכוללים פרטים אישיים על אודות נכי צה"ל דוגמת מספרם האישי בצה"ל, החיל שבו שירתו ודרגתם, כדי שתהיה אפשרות לשמור אותם ברשת הבלמ"סית. מכאן שלצד הצורך בשמירת מידע משנים עברו התאפשר להשמיט מהמאגר נתונים מסוימים.

בביקורת עלה כי שלא בהתאם לנדרש בתקנות אבטחת מידע כי בעל שליטה במאגר מידע יוודא אחת לשנה שהמידע השמור במאגר אינו רב מן הנדרש בהתאם למטרות המאגר, אגף התקשוב לא וידא זאת ולא הנחה את מנהלי האגפים והיחידות במשרד הביטחון שמשתמשים במאגרים לצורך עבודתם לבדוק זאת, מה שעלול להותיר במאגר מידע עודף שאין בו צורך. שמירת מידע עודף עלולה לפגוע בפרטיות משום שעלול להיעשות שימוש במידע זה שלא למטרות שלשמן הוא נאסף, לרבות העברתו לאחרים, עיבודו והצלבתו עם מידע נוסף. כך לדוגמה, במאגר נכי צה"ל, המשמש את אגף שיקום נכים בעבודתו, נשמרו פרטים אישיים בנוגע לשירות הצבאי של הנכים, לרבות החיל שבו שירתו ודרגתם, אף שלא היה בכך צורך.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-עמידה בבחינת מידע עודף אחת לשנה, זאת בסכום של 40,000 ש"ח לכל מאגר מידע ברמת אבטחה בינונית ו-160,000 ש"ח לכל מאגר מידע ברמת אבטחה גבוהה.

---

32 לפי סעיף 8(ב) לחוק.

33 לפי סעיף 2(ג) לתקנות.

34 הרשות להגנת הפרטיות, "צמצום מידע (Data Minimization) - מסמך מדיניות, טיוטה להערות הציבור", 25.3.21.

35 למאגרים האלה: נכי צה"ל, משפחות שכולות, חללים, פדויי שבי, צד"ל, עובדים ויועצים.

36 וכן כדי לאפשר לעובדים לעבוד מהבית בשעת חירום.

על ראש אגף התקשוב להנחות את ראשי האגפים וראשי היחידות במשרד הביטחון לבדוק אחת לשנה אם קיים מידע עודף בכל מאגרי המידע שבאגפיהם וביחידותיהם ולהסיר אותו וכן לתעד את ביצוע פעולותיהם. זאת מתוקף סמכותו כמנהל מאגרי המידע של משרד הביטחון ומתוקף אחריותו לעמידה בדרישות המנויות בתקנות.

מבנה המאגר ורשימת מצאי של מערכות המאגר

בעל שליטה במאגר מידע נדרש למפות את המערכות של מאגרי המידע ולהחזיק מסמך מעודכן בעניין מבנה מאגר המידע ורשימה מעודכנת בדבר המצאי של מערכות המאגר, ובכלל זה את הרכיבים המפורטים בתרשים שלהלן[37]:

תרשים 7: **מבנה מאגר המידע ורשימת מצאי של מערכות המאגר**

לפי תקנות אבטחת מידע, בעיבוד משרד מבקר המדינה.

מיפוי מערכות המאגר נועד להכיר את המידע הארגוני ולשלוט בו באמצעות שיקוף והצגה של מערכות המידע שבאמצעותן מעובד מידע מהמאגר, לרבות אמצעי האבטחה להגנת המערכות. מיפוי זה עשוי לסייע לארגון בהבנת המאפיינים הייחודיים של כל מאגר, התהליכים והממשקים בסביבת המחשוב של המאגרים, ומכאן גם חשיבותו בניהול סיכוני אבטחת המידע הנשקפים למאגר[38].

בפגישות שקיימו נציגי משרד מבקר המדינה בספטמבר ובאוקטובר 2024 עם נציגי היחידות לפיתוח היישומים המקושרים למאגרי מידע שונים[39] צוין כי קיימים מסמכי אפיון רבים למערכות המידע שבאמצעותן מעובדים נתוני המאגרים, שכוללים רמות פירוט שונות לרבות בנוגע לסוגי המידע שקיימים במערכות, לשדות ולפעולות שמתבצעות במערכות, להרשאות הקיימות, לסוגי הטבלאות וסוגי המסכים של המערכות ועוד. אולם אגף התקשוב לא מבצע מיפוי שוטף של מצאי המערכות של כל אחד ממאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם, ואין לאגף מסמך עדכני, סדור ומתכלל בנוגע למבנה מאגרי המידע ולמצאי המערכות כנדרש בתקנות.

בכתב המינוי של הממונה על אבטחת מידע באגף התקשוב מאוקטובר 2024 צוין כי אחד מתפקידיה הוא לבצע מיפוי של מערכות מאגרי המידע. בפגישה שקיימו נציגי משרד מבקר המדינה בנובמבר

37 לפי תקנה 5 לתקנות.
38 הרשות להגנת הפרטיות, נייר עמדה בנושא ביצוע סקר סיכונים ומבדק חדירות למערכות מידע.
39 למאגרים האלה: נכי צה"ל, משפחות שכולות, חללים, פדויי שבי, צד"ל, עובדים ויועצים.

2024 עם הממונה על אבטחת מידע היא מסרה כי החברה שתייעץ לאגף התקשוב בנושא הגנת הפרטיות תבצע מיפוי של מאגרי המידע.

בביקורת עלה כי בניגוד לנדרש בתקנות אבטחת מידע, שלפיהן בעל שליטה במאגר מידע ימפה את המערכות של מאגרי המידע ויחזיק מסמך מעודכן בעניין מבנה מאגר המידע ומצאי של מערכות המאגר, אגף התקשוב לא מיפה את המערכות של כל המאגרים שהוא בעל השליטה בהם; הוא לא החזיק במסמך עדכני, סדור ומתכלל בנוגע למבנה מאגרי המידע; ולא החזיק ברשימה מעודכנת בדבר מצאי המערכות של המאגרים, לרבות תשתיות, מערכות תוכנה, ממשקי תקשורת ותרשים רשת. היעדר שיקוף סדור, מתוכלל ומעודכן של מבנה המאגרים ומצאי מערכות המאגרים פוגע ביכולתו של אגף התקשוב להבין את המאפיינים הייחודיים של כל מאגר, את התהליכים ואת הממשקים בסביבת המחשוב של המאגרים, ולכן פוגע גם ביכולתו של אגף התקשוב לנהל את סיכוני אבטחת המידע הנשקפים למאגרים.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-עמידה בחובה למפות את מערכות המאגרים ולהחזיק במסמך עדכני בנוגע למבנה מאגרי המידע ומצאי מערכותיהם בסכום של 20,000 ש"ח לכל מאגר מידע ברמת אבטחה בינונית ו-80,000 ש"ח לכל מאגר מידע ברמת אבטחה גבוהה.

על אגף התקשוב למפות באופן עיתי את המערכות של מאגרי המידע ולהחזיק מסמך מבנה מאגר מעודכן ורשימה מעודכנת בדבר מצאי מערכות המאגר לכל אחד מהמאגרים שהוא בעל השליטה בהם. דבר זה יסייע לו לנהל את סיכוני אבטחת המידע הנשקפים למאגרים.

ניהול הרשאות הגישה למאגרי המידע

מערכות המחשוב של משרד הביטחון משולבות בכל תחומי הפעילות של המשרד, ובהתאם לכך יש אלפי בעלי תפקידים שלהם הרשאות גישה לרשתות המחשב, למערכות המידע ולמאגרי המידע המקושרים אליהן. לכל בעל תפקיד מוקצה קוד משתמש ייחודי (User) שלפיו מזוהות הרשאותיו למערכות המחשוב.

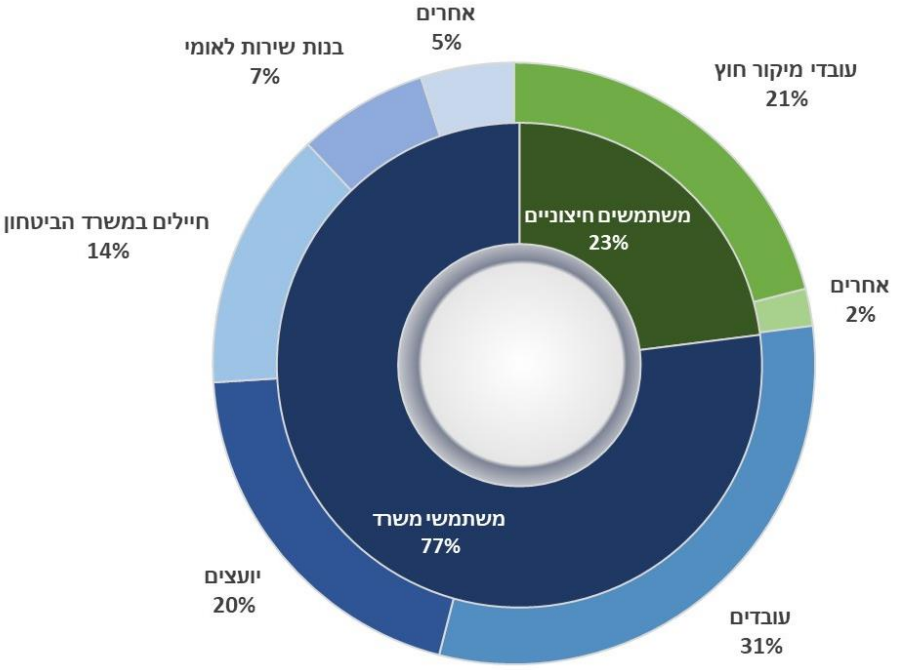
משתמשי מערכות המחשוב נחלקים לשתי קבוצות: (א) קבוצת משתמשי משרד - משתמשים שפרטיהם האישיים מנוהלים במערכות כוח האדם של משרד הביטחון, ובהם עובדי המשרד, יועצים, בנות שירות לאומי וחיילי צה"ל שמשרתים במשרד הביטחון; (ב) קבוצת המשתמשים החיצוניים - משתמשים שפרטיהם אינם מנוהלים במערכות כוח האדם של משרד הביטחון, ובהם עובדי מיקור חוץ, עובדי תעשיות ביטחוניות ומשתמשי צה"ל[40].

ניהול הרשאות גישה במערכת ניהול זהויות

אגף התקשוב מנהל במערכת ממוחשבת לניהול זהויות (להלן - מערכת ניהול זהויות) את זהויות המשתמשים משתי הקבוצות ואת תהליכי הבקשה והאישור של הרשאות הגישה שלהם למערכות המחשוב של משרד הביטחון, לרבות לרשתות ולמערכות מידע. להלן בתרשים התפלגות המשתמשים הפעילים במערכות המחשוב לפי קבוצות.

[40] בעלי תפקידים בצה"ל שמשתמשים במערכות המחשוב של משרד הביטחון לצורך מילוי תפקידם.

תרשים 8: **התפלגות המשתמשים הפעילים במערכות המחשוב של משרד הביטחון**



על פי נתוני מערכת ניהול זהויות של משרד הביטחון מנובמבר 2024, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מרבית המשתמשים הפעילים במערכות המחשוב של משרד הביטחון (77%) הם מקבוצת משתמשי משרד שפרטיהם מנוהלים במערכות כוח האדם של משרד הביטחון, ובהם עובדים (31% מסך המשתמשים הפעילים), יועצים (20%) וחיילים המשרתים במשרד הביטחון (14%). כרבע מהמשתמשים הפעילים (23%) הם מקבוצת המשתמשים החיצוניים, מרביתם עובדי מיקור חוץ.

גורמים שונים עוסקים בניהול ההרשאות: (א) גורמים דורשים, שהם בעלי תפקידים מטעם אגפי משרד הביטחון וצה"ל המורשים לפנות לאגף התקשוב בבקשה למתן הרשאות ולביטולן הן עבור קבוצת משתמשי משרד והן עבור קבוצת המשתמשים החיצוניים; (ב) יחידת תחום הרשאות באגף התקשוב שתפקידה להקים חשבונות למשתמשים חדשים ולתת הרשאות גישה במערכת ניהול זהויות; (ג) יחידת תחום פיתוח מערכות באגף התקשוב שאחראית לבניית ההרשאות במערכת ניהול זהויות.

ביטול הרשאות במערכת ניהול זהויות עם סיום תפקידו של בעל ההרשאה

בעת סיום התפקיד של משתמש מקבוצת משתמשי משרד, יחידת תחום הרשאות מקבלת עדכון אוטומטי ישירות למערכת ניהול זהויות ממערכת המידע של אגף משאבי אנוש ומבטלת את ההרשאות בהתאם במערכת ניהול זהויות. לעומת זאת, בעת סיום תפקיד של משתמש מקבוצת המשתמשים החיצוניים נדרש הגורם הדורש לעדכן בדואר אלקטרוני את יחידת תחום הרשאות על שינוי הסטטוס של המשתמש, ובהתאם לעדכונים אלה יחידת תחום הרשאות מבטלת את ההרשאות במערכת ניהול זהויות.

בפגישה שקיימו נציגי משרד מבקר המדינה עם ראש התחום לפיתוח מערכות בספטמבר 2024 הוא מסר כי מכיוון שאין מנגנון דיווח אוטומטי שבו הגורמים הדורשים באגפי משרד הביטחון ובצה"ל מעדכנים את אגף התקשוב על סיום תפקידם של משתמשים מקבוצת המשתמשים החיצוניים,

במקרים רבים האגף אינו מקבל עדכון, ולכן ההרשאות של משתמשים אלו במערכת ניהול זהויות נותרות פעילות שלא לצורך, ובכלל זה הרשאות לרשתות ולמערכות מידע שהן שער הכניסה למאגרי המידע. למשל, במקרים מסוימים צה"ל אינו מדווח לאגף התקשוב על שינויים בסטטוס של חיילים, כגון שינוי תפקיד או שחרור מצה"ל, וכתוצאה מכך ייתכן שחייל שקיבל הרשאות למערכות המידע של משרד הביטחון החליף תפקיד ולא נדרש יותר להרשאות שקיבל לצורך מילוי תפקידו, אך עדיין יש לו הרשאות גישה וצפייה ואף הרשאות לביצוע פעולות במערכות המידע של משרד הביטחון.

בביקורת עלה כי אגף התקשוב במשרד הביטחון לא הסדיר שיטת דיווח מצד הגורמים דורשי ההרשאות מאגפי משרד הביטחון וצה"ל בנוגע לסיום תפקידם של משתמשים מקבוצת המשתמשים החיצוניים לצורך ביטול הרשאותיהם. זאת אף שכתוצאה מהיעדר דיווח סדור קיימות הרשאות פעילות שלא לצורך בקבוצת המשתמשים החיצוניים, ובכלל זה הרשאות לרשתות מחשבים ולמערכות מידע שהן שער כניסה למאגרי מידע.

על אגף התקשוב לקבוע שיטה לדיווח סדור בנוגע לסיום תפקידם של קבוצת המשתמשים החיצוניים מצד הגורמים הדורשים באגפי משרד הביטחון ובצה"ל. זאת כדי שאגף התקשוב יוכל לבטל במערכת ניהול זהויות את ההרשאות, ובכלל זה הרשאות לרשתות ולמערכות מידע שהן שער כניסה למאגרי מידע, שאינן נחוצות למשתמשים מקבוצה זו מיד עם סיום תפקידם.

במטרה לבחון את פוטנציאל הסיכון הטמון בכך שאגף התקשוב אינו מבטל הרשאות של משתמשים חיצוניים מיד עם סיום תפקידם בשל היעדר דיווח סדור, ניתח משרד מבקר המדינה את מועד הכניסה (Log-in) האחרון של המשתמשים החיצוניים לרשת מרכזית מסוימת במשרד הביטחון וכן את שיוכם האגפי, על סמך מידע שהעביר לו אגף התקשוב ממערכת ניהול זהויות נכון לדצמבר 2024. מועד הכניסה האחרון של המשתמש לרשת עשוי להצביע על נחיצות הרשאת הגישה שלו לרשת לצורך ביצוע תפקידו.

יודגש כי ברשת זו קיימים נכסים, חלקם רגישים, וכן תשומות המשרתים תהליכים עסקיים ותהליכי הצטיידות של צה"ל, והיא מתפרסת על פני אתרים שונים בארץ ובעולם.

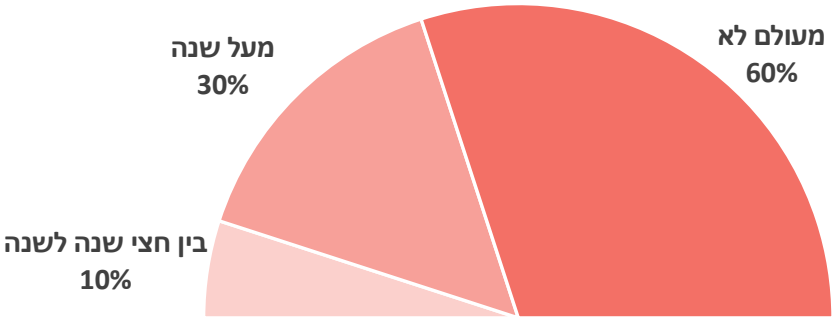
להלן תרשימים שמציגים את עיקרי הממצאים שעלו בבדיקה:

תרשים 9: **שיעור המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה מכלל המשתמשים החיצוניים בעלי הרשאת גישה פעילה לרשת**

על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 7 מכל 10 משתמשים חיצוניים בעלי הרשאת גישה פעילה לרשת מרכזית של משרד הביטחון לא נכנסו לרשת זו יותר מחצי שנה, ובהם משתמשים שלא נכנסו אליה מעולם.

תרשים 10: **התפלגות מועד הכניסה האחרון של המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה**

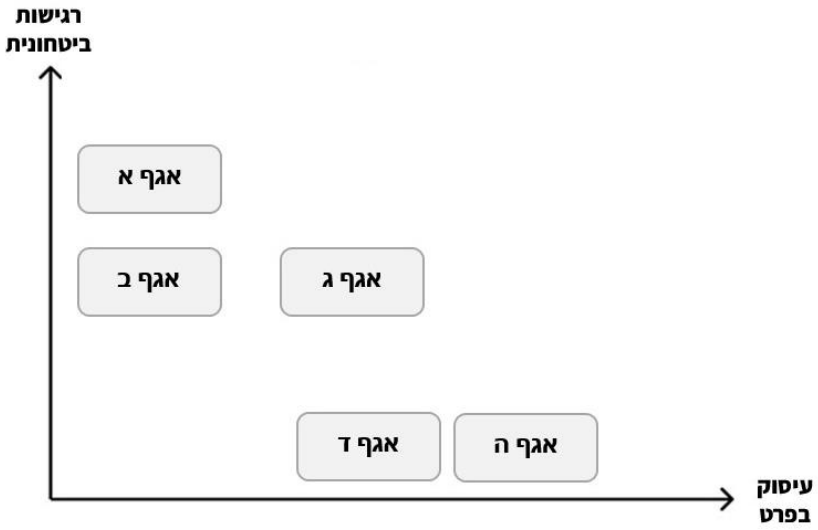


על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מתוך המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה - 60% לא נכנסו אליה מעולם, ו-40% נכנסו אליה בעבר. כמו כן 30% לא נכנסו לרשת יותר משנה, ו-10% לא נכנסו לרשת בין חצי שנה לשנה. יצוין כי 90% מהמשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה הם עובדי מיקור חוץ.

עוד עלה בבדיקה כי 60% מכלל המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה (כולל אלו שלא נכנסו אליה מעולם) משויכים לחמישה אגפים במשרד הביטחון. להלן מוצגים חמשת האגפים שאליהם משויכים מרבית המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה לפי מידת רגישותם הביטחונית ועיסוקם בפרט.

תרשים 11: **חמשת האגפים שאליהם משויכים מרבית המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה לפי מידת רגישותם הביטחונית ועיסוקם בפרט**



על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי שלושה מתוך חמשת האגפים שאליהם משויכים מרבית המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה הם אגפים שמידת הסיכון לחשיפת מידע ביטחוני מתוכם היא גבוהה; ושלושה אגפים מתוך החמישה הם אגפים שמידת הסיכון לחשיפת מידע בנוגע לפרט מתוכם היא גבוהה. יצוין כי בארבעה מתוך חמשת האגפים מדובר במספר משתמשים הגדול מ-100.

בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה, 7 מכל 10 משתמשים חיצוניים בעלי הרשאת גישה לרשת מחשב מרכזית של משרד הביטחון, שהיא שער כניסה למאגרי מידע, לא נכנסו לרשת זו יותר מחצי שנה, מרביתם (60%) לא נכנסו אליה מעולם. במצב זה עולה חשש כי הם בעלי הרשאת גישה שלא לצורך ביצוע תפקידם. עוד עלה כי מרבית המשתמשים שלא נכנסו לרשת יותר מחצי שנה (90%) הם עובדי מיקור חוץ, וחלק גדול מהם (60%) משויכים לחמישה אגפים שמידת הסיכון לחשיפה של מידע ביטחוני מתוכם או של מידע בנוגע לפרט מתוכם, היא גבוהה. מאחר שרשת זו היא שער הכניסה למאגרי מידע, וקיימים בה נכסים, חלקם רגישים, וכן תשומות המשרתים תהליכים עסקיים ותהליכי הצטיידות של צה"ל, גובר הסיכון לחשיפת מידע רגיש בפני מי שאינם מורשים לכך.

על אגף התקשוב לבדוק באופן עיתי את ההרשאות של המשתמשים החיצוניים במערכת ניהול זהויות ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם. זאת נוכח הממצאים שהעלה משרד מבקר המדינה, המעלים חשש כי קיימים משתמשים חיצוניים רבים שלהם הרשאות גישה שאינן נחוצות לצורך ביצוע תפקידם, וייתכן כי הדבר נובע מאי-דיווח על סיום תפקידם.

בתגובתו על ממצאי הביקורת ציין משרד הביטחון כי בוצעה "הקפאה/מחיקה" של הרשאות של אלפי משתמשים בלתי פעילים.

הבקרה על הרשאות הגישה במערכת ניהול זהויות

בעל השליטה במאגר מידע נדרש לנהל רישום מעודכן של תפקידים (Role), של הרשאות הגישה הנדרשות לביצוע תפקידים אלה ושל בעלי ההרשאות (משתמשים) הממלאים תפקידים אלה[41].

אחד הכלים המקובלים לניהול הרשאות משתמשים הוא ביצוע סקירת הרשאות סדורה ותקופתית של חשבונות המשתמשים הפעילים וההרשאות שניתנו להם, המסייעת בזיהוי משתמשים שסיימו את תפקידם או שעזבו את הארגון, בטיוב ההרשאות הקיימות, בביטול הרשאות ותפקידים מיותרים ובמניעת פערי אבטחה אפשריים. לביצוע סקירת הרשאות במשרד הביטחון באופן סדור, מובנה ועיתי של חשבונות המשתמשים והרשאות הגישה הניתנות להם במסגרת תפקידם, יש משנה חשיבות נוכח היעדרה של שיטת דיווח סדורה בנוגע לסיום תפקידם של משתמשים חיצוניים למשרד הביטחון, דבר שמגביר את הסיכון לחשיפת מידע מוגן בפני מי שאינם מורשים לכך.

ראש התחום לפיתוח מערכות, האחראי בין היתר על מערכת ניהול זהויות במשרד הביטחון, מבצע בדיקות יזומות של הרשאות מפעם לפעם כדי לבדוק אם משתמשים המופיעים כפעילים במערכת אינם פעילים עוד ונדרש לבטל להם את הרשאות הגישה הקיימות. אולם, בדיקות אלה מתמקדות בכל פעם בקבוצת משתמשים מצומצמת (עשרות עד מאות בודדות מתוך אלפי חשבונות משתמשים פעילים) ומתבצעות באופן ידני ועל פי שיקול דעתו[42].

לדברי ראש התחום לפיתוח מערכות מספטמבר 2024, לא מתבצעת סקירת הרשאות עיתית, סדורה ומובנית לכלל ההרשאות והמשתמשים. זאת משום שבמערכת ניהול זהויות מנוהלים עשרות אלפי משתמשים, פעילים ושאינם פעילים, וכן עשרות אלפי סוגי הרשאות, והנתונים בה הם דינמיים, ולכן יש אתגר בביצוע בקרה סדורה על ההרשאות. עוד הוא ציין כי הוא אינו מקבל

---

41 לפי תקנה 8(ב) לתקנות.

42 יצוין כי בגופים שונים מתבצעת סקירת הרשאות סדורה, עיתית וממוחשבת. לדוגמה, בחברת דואר ישראל קיים נוהל המנחה על ביצוע סקירת הרשאות ומסדיר את הטיפול בממצאים. כמו כן, החברה מבצעת פעמיים בשנה סקירת הרשאות ידנית ומדי חודש בדיקת הרשאות ממוחשבת לאיתור עובדים שעזבו את החברה אך הרשאותיהם טרם בוטלו (מבקר המדינה, **דוח מבקר המדינה - נובמבר 2024**, "מערכות המידע בחברת דואר ישראל ובבנק הדואר", עמ' 38).

פניות ממנהלי פרויקטים באגף התקשוב, ממנהלי קשרי לקוחות באגף או מגורמים רלוונטיים אחרים בבקשה להפיק דוחות על ההרשאות לצורכי בדיקה פנימית שלהם.

בביקורת עלה כי אגף התקשוב אינו מבצע סקירת הרשאות סדורה ומובנית על אלפי המשתמשים המנוהלים במערכת ניהול זהויות ועל עשרות אלפי סוגי ההרשאות שבה לצורך עדכון רשימות המשתמשים, אלא הוא מבצע מפעם לפעם בדיקות ממוקדות של הרשאות לקבוצת משתמשים מצומצמת לפי שיקול דעתו ובאופן ידני. זאת, שלא בהתאם לדרישה בתקנות לנהל רישום מעודכן של המשתמשים ושל הרשאות הגישה שניתנו להם לביצוע תפקידם ואף שאגף התקשוב מודע לקיומן של הרשאות שאינן לצורך בקבוצת המשתמשים החיצוניים.

על אגף התקשוב לקבוע מנגנון סדור ועיתי לביצוע סקירת הרשאות סדורה במערכת ניהול זהויות שתסייע לו לוודא כי קיימות הרשאות פעילות למשתמשים מורשים בלבד בהתאם לצורכיהם וכן תאפשר לו לטייב את רשימת ההרשאות ולנהל רישום מעודכן של התפקידים, של הרשאות הגישה הנדרשות לביצוע תפקידים אלה ושל בעלי ההרשאות הממלאים תפקידים אלה, כנדרש בתקנות אבטחת מידע.

נוסף על ניתוח נתוני קבוצת המשתמשים החיצוניים, שלגביהם אגף התקשוב מודע לקיומן של הרשאות פעילות שלא לצורך, ניתח משרד מבקר המדינה גם את מועד הכניסה (Log-in) האחרון של קבוצת משתמשי משרד לנוכח הממצאים שעלו בנוגע לקבוצת המשתמשים החיצוניים. כאמור, בעת סיום תפקיד של משתמש מקבוצת משתמשי משרד, יחידת תחום הרשאות מקבלת עדכון אוטומטי ישירות למערכת ניהול זהויות ממערכת המידע של אגף משאבי אנוש ונדרשת לבטל את ההרשאות במערכת ניהול זהויות בהתאם.

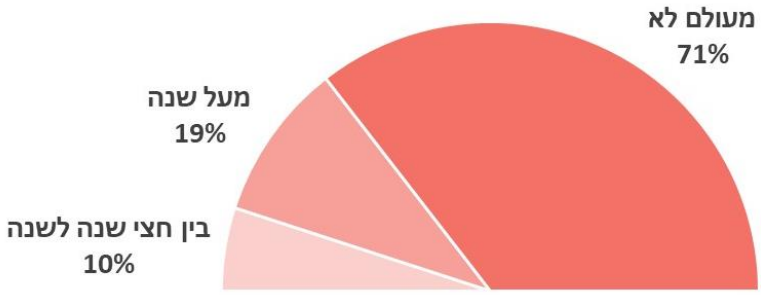
להלן תרשימים שמציגים את עיקרי הממצאים שעלו בבדיקה בהתייחס לקבוצת משתמשי משרד.

תרשים 12: **שיעור משתמשי משרד שלא נכנסו לרשת יותר מחצי שנה מכלל משתמשי משרד בעלי הרשאת גישה פעילה לרשת**

על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 3 מכל 10 משתמשי משרד בעלי הרשאת גישה פעילה לרשת מרכזית של משרד הביטחון לא נכנסו לרשת זו יותר מחצי שנה, ובהם משתמשים שלא נכנסו אליה מעולם.

תרשים 13: **התפלגות מועד הכניסה האחרון של משתמשי משרד שלא נכנסו לרשת יותר מחצי שנה**



על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מתוך קבוצת משתמשי משרד שלא נכנסו לרשת יותר מחצי שנה - 71% לא נכנסו אליה מעולם, ו-29% נכנסו אליה בעבר. כמו כן 19% לא נכנסו לרשת יותר משנה, ו-10% לא נכנסו לרשת בין חצי שנה לשנה.

עוד עלה בבדיקה כי מתוך קבוצת משתמשי משרד שלא נכנסו לרשת יותר מחצי שנה - רובם (85%) אינם עובדי משרד הביטחון, ובהם יועצים (37%), חיילים שמשרתים במשרד הביטחון (31%) ובנות שירות לאומי (9%). 15% מקבוצת משתמשי המשרד שלא נכנסו לרשת יותר מחצי שנה הם עובדי המשרד.

עוד עלה בבדיקה כי 75% מקבוצת משתמשי משרד שלא נכנסו לרשת יותר מחצי שנה (כולל אלו שלא נכנסו אליה מעולם) משויכים לעשרה אגפים במשרד הביטחון ובהם אגפים שמידת הסיכון לחשיפה של מידע ביטחוני או מידע בנוגע לפרט מתוכם היא גבוהה. יצוין כי מספרם של משתמשים אלו הוא בין עשרות למאות בכל אגף, ובמצב זה גובר הסיכון לחשיפת מידע אישי בפני מי שאינם מורשים לכך.

בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה, גם בקבוצת משתמשי משרד קיימים בעלי הרשאת גישה פעילה לרשת מרכזית מסוימת במשרד הביטחון שלא נכנסו לרשת זו יותר מחצי שנה (3 מכל 10 משתמשים בקבוצה), מרביתם (71%) לא נכנסו אליה מעולם. עוד עלה מהניתוח כי מרבית משתמשים אלה (85%) אינם עובדי משרד הביטחון, ובהם יועצים (37%), חיילים שמשרתים במשרד הביטחון (31%) ובנות שירות לאומי (9%). 15% מהם הם עובדי משרד. נוסף על כך, יש בקבוצה זו משתמשים שמשויכים לאגפים שמידת הסיכון לחשיפה של מידע ביטחוני מתוכם או של מידע בנוגע לפרט מתוכם היא גבוהה. במצב זה גובר הסיכון לחשיפת מידע רגיש בפני מי שאינם מורשים לכך.

על אגף התקשוב לבדוק גם את ההרשאות של משתמשי משרד במערכת ניהול זהויות ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם. זאת נוכח הממצאים שהעלה משרד מבקר המדינה המעלים חשש כי גם בקרב קבוצת משתמשי משרד קיימים משתמשים שלהם הרשאות גישה שאינן נחוצות להם לצורך ביצוע תפקידם.

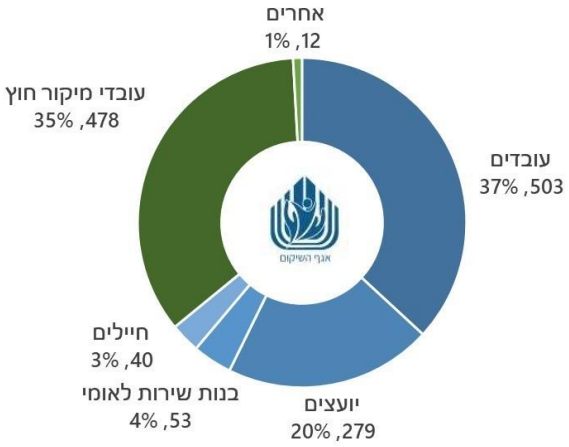
בתגובתו על ממצאי הביקורת ציין משרד הביטחון כי במשרד מוקמת מערכת חדשה לניהול זהויות שבה ייושמו המתודולוגיה והרגולציה הנדרשות.

ניהול הרשאות הגישה למאגר נכי צה"ל

נוסף על בדיקת ניהול ההרשאות במערכת ניהול זהויות, ובכלל זה הרשאות לרשתות ולמערכות מידע שהן שערי הכניסה למאגרי המידע של משרד הביטחון, בדק משרד מבקר המדינה את ניהול ההרשאות במערכת שמש (מערכת המידע המרכזית של אגף שיקום נכים) המקושרת למאגר המידע של נכי צה"ל[43]. זאת נוכח רגישות המידע הקיים במאגר זה, המכיל מידע אישי בנוגע ליותר מ-230,000 אנשים[44], לרבות פרטים על מצבם הבריאותי, מצבם הכלכלי, בני משפחותיהם, השירותים הניתנים להם ועוד, וכן נוכח תוספת של כ-18,000 פצועים שפנו לאגף שיקום נכים[45] ונוספו למאגר נכי צה"ל בשל מלחמת חרבות ברזל והגידול בעקבות זאת במספר המשתמשים במערכת שמש. יודגש כי מאגר נכי צה"ל מסווג ברמת אבטחה גבוהה לפי תקנות אבטחת מידע. כלומר, סיכוני האבטחה הנשקפים למאגר זה הם ברמה הגבוהה ביותר.

במערכת שמש קיימת מערכת ניהול הרשאות פנימית המאפשרת גישה למאגר נכי צה"ל ובה מנוהלים 1,365 משתמשים פעילים בעלי הרשאות גישה. להלן בתרשים התפלגות המשתמשים הפעילים בעלי הרשאות גישה למערכת שמש.

תרשים 14: **התפלגות המשתמשים הפעילים בעלי הרשאות גישה למערכת שמש שאליה מקושר מאגר המידע של נכי צה"ל**



על פי נתוני הרשאות של משרד הביטחון מינואר 2025, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מרבית המשתמשים בעלי הרשאות גישה למערכת שמש שאליה מקושר מאגר המידע של נכי צה"ל הם מקבוצת משתמשי משרד (65%), ובהם יותר משליש עובדי משרד הביטחון (37% מסך המשתמשים הפעילים), כחמישית יועצים (20%) והיתר בנות שירות לאומי (4%), חיילים (3%) ואחרים (1%). עוד עלה כי יותר משליש מהמשתמשים הפעילים במערכת שמש (35%) הם עובדי מיקור חוץ מקבוצת המשתמשים החיצוניים.

ביטול הרשאות הגישה למאגר נכי צה"ל עם סיום תפקידו של בעל ההרשאה

ראש היחידה לניהול קשרי לקוחות של אגף התקשוב באגף שיקום נכים אמון על ניהול ההרשאות במערכת שמש בהתאם לדרישה מבעל תפקיד בכיר באגף שיקום נכים המורשה לאשר הרשאות.

---

43 המערכת משמשת גם את אגף משפחות, הנצחה ומורשת במשרד הביטחון ומקושרת למאגרי מידע נוספים כגון מאגר משפחות שכולות ומאגר חללי צה"ל.

44 לרבות נכי צה"ל שנפטרו ולרבות נפגעים שפנו לאגף שיקום נכים בבקשה להכרה בנכות ולא הוכרו.

45 מספר הפניות בבקשה להכרה בנכות מאוקטובר 2023 עד ספטמבר 2024, לפי נתוני אגף שיקום נכים.

בפגישה שקיימו נציגי משרד מבקר המדינה עם ראש היחידה לניהול קשרי לקוחות באוקטובר 2024 הוא מסר כי כאשר משתמש מקבוצת משתמשי משרד מסיים את עבודתו, הגישה שלו לרשת שבה נמצאת מערכת שמש נחסמת אוטומטית במערכת ניהול זהויות. כאשר משתמש מקבוצת המשתמשים החיצוניים מסיים את עבודתו, נדרשת אמרכלות אגף שיקום נכים, שאחראית בין היתר על ניהול פרטיהם של קבוצת המשתמשים החיצוניים, לעדכן את ראש היחידה על כך, ובהתאם הוא מבטל את ההרשאות במערכת שמש. אולם, קיימים מקרים שבהם אמרכלות אגף שיקום נכים אינה מעדכנת אותו על סיום תפקיד, והרשאות הגישה של המשתמש החיצוני למערכת שמש ולמאגר נכי צה"ל נשארות פעילות. מקרים אלה מתרחשים בעיקר בנוגע לעובדים המועסקים באמצעות ספק חיצוני, דוגמת המוקד הטלפוני של אגף שיקום נכים[46] המונה עשרות עובדים. כמו כן, יש ספקים חיצוניים שיכולים לעבוד מרחוק, ובמצב שבו אמרכלות האגף אינה מעודכנת על סיום תפקידם הרשאותיהם נותרות פעילות, ויש להם גישה למערכת שמש שאליה מקושר מאגר המידע של נכי צה"ל. בכך יש סיכון גבוה שמשתמשים בלתי מורשים יחזיקו בהרשאה שלא לצורך.

בביקורת עלה כי אגף התקשוב במשרד הביטחון לא הסדיר שיטת דיווח מצד הגורמים דורשי ההרשאות בנוגע לסיום תפקידם של משתמשים חיצוניים במערכת שמש, שאליה מקושר מאגר המידע של נכי צה"ל, לצורך ביטול הרשאותיהם. זאת אף שעקב היעדר דיווח סדור קיימות הרשאות פעילות שלא לצורך למערכת שמש בקבוצת המשתמשים החיצוניים. לדוגמה, היו הרשאות פעילות שלא לצורך לעובדים שהועסקו באמצעות ספק חיצוני, דוגמת המוקד הטלפוני של אגף שיקום נכים שמונה עשרות עובדים ומתאפיין בתחלופה של עובדים, וכן לספקים חיצוניים שיכלו להתחבר מרחוק למערכת שמש, וזאת אף שהם סיימו את תפקידם.

כתוצאה מכך, בנסיבות מסוימות עלולים גורמים בלתי מורשים להיחשף למידע אישי לרבות מידע בעל רגישות מיוחדת במאגר נכי צה"ל שכולל פרטים על אודות יותר מ-230,000 אנשים, ובכלל זה מצבם הבריאותי, מצבם הכלכלי, בני משפחותיהם והשירותים הניתנים להם. סיכון זה גובר נוכח הגידול של כ-18,000 פצועים שנוספו למאגר נכי צה"ל בשל מלחמת חרבות ברזל והגידול בעקבות זאת במספר נותני השירותים באגף שיקום נכים המשתמשים במערכת שמש.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-ביטול הרשאות גישה למשתמשים מיד עם סיום תפקידם בסכום של 160,000 ש"ח למאגר ברמת אבטחה גבוהה, דוגמת מאגר נכי צה"ל.

על אגף התקשוב לקבוע שיטה לדיווח סדור בנוגע לסיום תפקידם של משתמשים בעלי הרשאה למערכת שמש שתאפשר לאגף לבטל את הרשאותיהם מיד עם סיום תפקידם ובהתאם לפעול לביטול ההרשאות.

כדי לבחון את פוטנציאל הסיכון הטמון בכך שאגף התקשוב אינו מבטל הרשאות של משתמשים חיצוניים למערכת שמש מיד עם סיום תפקידם בשל היעדר דיווח סדור, ניתח משרד מבקר המדינה את נתוני המשתמשים החיצוניים במערכת שמש על סמך מידע שהעביר לו אגף התקשוב נכון לינואר 2025. התרשימים שלהלן מציגים את עיקרי הממצאים שעלו בניתוח בהתייחס לקבוצת המשתמשים החיצוניים שהם בעלי הרשאת גישה פעילה למערכת שמש על פי מועד הכניסה (Log-in) האחרון שלהם למערכת.

---

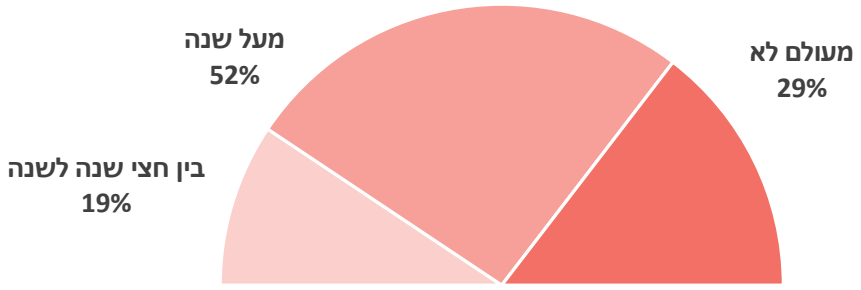
[46] עובדי המוקד הטלפוני מוגדרים משתמשים חיצוניים, וקבוצה זו מאופיינת בתחלופה רבה מאחר שרובם סטודנטים המועסקים בעבודה זמנית.

תרשים 15: **שיעור המשתמשים החיצוניים שלא נכנסו למערכת שמש יותר מחצי שנה מכלל המשתמשים החיצוניים בעלי הרשאת גישה פעילה**

על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 5 מכל 10 משתמשים חיצוניים בעלי הרשאת גישה פעילה למערכת שמש לא נכנסו למערכת יותר מחצי שנה ובהם, משתמשים שלא נכנסו אליה מעולם. מדובר ב-263 משתמשים שלא נכנסו למערכת יותר מחצי שנה מתוך 481 משתמשים חיצוניים בעלי הרשאת גישה פעילה למערכת שמש.

תרשים 16: **התפלגות מועד הכניסה האחרון למערכת שמש של משתמשים חיצוניים שלא נכנסו למערכת יותר מחצי שנה**



על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי מתוך המשתמשים החיצוניים שלא נכנסו למערכת שמש יותר מחצי שנה - 29% לא נכנסו אליה מעולם, ו-71% נכנסו אליה בעבר. כמו כן 52% לא נכנסו למערכת יותר משנה, ו-19% לא נכנסו למערכת בין חצי שנה לשנה.

בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה לנתוני קבוצת המשתמשים החיצוניים במערכת שמש, שאליה מקושר מאגר המידע של נכי צה"ל, 5 מכל 10 משתמשים בעלי הרשאת גישה פעילה למערכת (263 משתמשים מתוך 481) לא נכנסו למערכת זו יותר מחצי שנה, חלקם (29% מהם, שהם 78 משתמשים) לא נכנסו אליה מעולם. במצב זה עולה חשש כי הם בעלי הרשאת גישה שלא לצורך ביצוע תפקידם.

על אגף התקשוב לבדוק באופן עיתי את ההרשאות של המשתמשים החיצוניים במערכת שמש ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם.

הבקרה על הרשאות הגישה למאגר נכי צה"ל

ראש היחידה לניהול קשרי לקוחות של אגף התקשוב באגף שיקום נכים מבצע בקרה יזומה על הרשאות הגישה של המשתמשים במערכת שמש כאשר הוא מזהה חריגות בהרשאות של בעלי תפקידים. כמו כן, מדי חודש הוא מבצע בקרה על הרשאה מסוג מנהל מערכת, שהיא הרשאה חזקה שמאפשרת לתת הרשאות למשתמשים אחרים ואף לחתום בשמם של בעלי תפקידים מסוימים.

אולם, לדבריו כפי שנמסרו למשרד מבקר המדינה באוקטובר 2024, הוא אינו מקיים בקרה סדורה על כלל ההרשאות במערכת שמש.

בביקורת עלה כי אגף התקשוב אינו מבצע סקירת הרשאות סדורה ומובנית לגבי כלל המשתמשים במערכת שמש, שאליה מקושר מאגר נכי צה"ל, והוא אינו מנהל רישום מעודכן של המשתמשים ושל הרשאות הגישה שניתנו להם לביצוע תפקידם, כנדרש בתקנות. עקב כך עלולים להיות משתמשים שהם בעלי הרשאות גישה שלא לצורך, דבר שמגביר את הסיכון לחשיפת מידע אישי, לרבות מידע בעל רגישות מיוחדת, בפני מי שאינם מורשים לכך.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין רישום לא מעודכן של תפקידים, של הרשאות ושל משתמשים במאגר מידע ברמת אבטחה גבוהה בסכום של 160,000 ש"ח, דוגמת מאגר נכי צה"ל.

מומלץ כי האגף יפתח מנגנון לביצוע סקירת הרשאות סדורה במערכת שמש שתסייע לו לנהל רישום מעודכן של תפקידים, של הרשאות הגישה הנדרשות לביצוע תפקידים אלה ושל בעלי ההרשאות הממלאים תפקידים אלה, כנדרש בתקנות. בכך הוא יוודא שהרשאות הגישה לפרטיהם האישיים והרגישים של נכי צה"ל יהיו רק בידי הגורמים המורשים לכך לצורך ביצוע תפקידם.

נוסף על ניתוח נתוני קבוצת המשתמשים החיצוניים במערכת שמש, שלגביהם אין דיווח אוטומטי וסדור בנוגע לסיום תפקידם, ניתח משרד מבקר המדינה גם את מועד הכניסה (Log-in) האחרון של קבוצת משתמשי משרד למערכת.

בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה, גם בקבוצת משתמשי משרד קיימים בעלי הרשאת גישה פעילה למערכת שמש, המקושרת למאגר נכי צה"ל; שיעורם של אלה שלא נכנסו למערכת שמש יותר מחצי שנה (ובהם אלו שלא נכנסו אליה מעולם) היה 22% מסך כל המשתמשים שלא נכנסו למערכת - שהם 75 משתמשים מתוך 338, מרביתם (88%, שהם 66 משתמשים) יועצים שמנוהלים במערכות כוח האדם של משרד הביטחון בדומה לעובדי המשרד. יצוין כי היחידות באגף שיקום נכים שבהן נמצא המספר הגבוה ביותר של יועצים שלא נכנסו למערכת שמש יותר מחצי שנה הן יחידת סגן בכיר לנושאי שירות (13 יועצים), יחידת סגן וראש היחידה למחקר, תכנון ותיאום (10 יועצים), ויחידת ועדות רפואיות (5 יועצים).

על אגף התקשוב לבחון את כלל ההרשאות הקיימות במערכת שמש ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם.

☆

בדוח זה תוארו ליקויים בנוגע לניהול הרשאות המשתמשים הן במערכת ניהול זהויות שבה מנוהלות ההרשאות לשערי הכניסה למאגרי המידע (לרשתות המחשבים ולמערכות מידע), והן במערכת שמש שבה מנוהלות ההרשאות למאגר נכי צה"ל, ובהם אלה: יותר ממחצית מהמשתמשים החיצוניים בעלי הרשאת גישה לא נכנסו יותר מחצי שנה לרשת מרכזית במשרד הביטחון ולמערכת שמש; אגף התקשוב לא הסדיר שיטת דיווח בנוגע לסיום תפקידם של המשתמשים החיצוניים לצורך ביטול הרשאותיהם, והוא אינו מבצע סקירת הרשאות סדורה ומובנית כדי לוודא שהרשאות הגישה יהיו רק בידי הגורמים המורשים לכך. לנוכח הליקויים שתוארו בדוח על אגף התקשוב לבדוק את כלל ההרשאות הקיימות ביתר מערכות המידע שמקושרות למאגרי המידע במשרד הביטחון ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם. כמו כן, מומלץ כי אגף התקשוב יבדוק גם את תהליכי ניהול ההרשאות ביתר מערכות המידע. דבר זה יסייע לו לצמצם את הסיכון לחשיפת מידע אישי, לרבות מידע בעל רגישות מיוחדת, בפני מי שאינם מורשים לכך, וכן לצמצם את הסיכון לדלף של מידע זה, לפגיעה

בזמינותו ולשיבושו; ובכך יפחת הסיכון לפגיעה בפרטיותם של האנשים שמידע אישי לגביהם שמור במאגרי המידע.

אבטחת המידע במאגרי המידע

אבטחת מידע היא מרכיב מהותי בהגנה מפני פגיעה בפרטיות המידע שבמאגר מידע. אבטחת מידע מוגדרת בחוק הגנת הפרטיות כהגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד בלא רשות כדין[47].

אגף התקשוב נושא באחריות לאבטחת המידע שבמאגרי המידע של משרד הביטחון. אולם, הגורם המקצועי ובעל הסמכות בתחום אבטחת מידע במשרד הביטחון הוא אגף ביטחון. האגף פועל מכוח החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, כגוף המונחה על ידי הממונה על הביטחון במערכת הביטחון (להלן - מלמ"ב). לפי הוראת ארגון אגף ביטחון, האגף מופקד על הביטחון ועל האבטחה של כלל אגפי המשרד, ובין תפקידיו לקבוע הוראות, הנחיות ונהלים ביטחוניים במשרד הביטחון ולבצע בקרה אחר יישומם; לבצע הגנה בסייבר על נכסי התקשוב, הטכנולוגיה ורשתות המחשב של משרד הביטחון; להגן על תשתיות ועל נכסי משרד הביטחון מפני חדירה, חבלה וחשיפת מידע; לבצע פיקוח ביטחוני על ספקי המשרד ועוד.

יודגש כי בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, שמכוחו פועל אגף ביטחון, מוגדרות פעולות לאבטחת מידע כפעולות הדרושות לשם שמירה על מידע מסווג, ואין בחוק התייחסות להיבטי הגנת הפרטיות.

משרד מבקר המדינה בחן את האופן שבו משרד הביטחון עמד בדרישות החלות עליו בתחום אבטחת המידע במאגרי המידע שהוא בעל השליטה בהם בהיבטי הגנת הפרטיות. זאת, על רקע המצב שבו אגף התקשוב נושא באחריות לאבטחת המידע שבמאגרי המידע של משרד הביטחון בהיבט הגנת הפרטיות, אולם הגורם המקצועי ובעל הסמכות בתחום אבטחת מידע במשרד הביטחון הוא אגף ביטחון, והוא זה שמבצע פעולות לאבטחת מידע הדרושות לשם שמירה על מידע מסווג, כפי שיפורט בשלושת תתי-הפרקים שלהלן:

1. נוהל אבטחה

בעל שליטה במאגר מידע נדרש לקבוע נוהל אבטחה[48] שמטרתו לייצר מדיניות אבטחה ארגונית להתמודדות עם סיכוני האבטחה שלהם חשוף המידע; ולשמש כלי לעריכת ביקורות תקופתיות לווידוא קיומם של אמצעי האבטחה הנדרשים ותקינותם[49]. את נוהל האבטחה יכין הממונה על אבטחת המידע ויביאו לאישור בעל השליטה במאגר[50]. על נוהל האבטחה של מאגרי מידע שחלה עליהם רמת אבטחה בינונית או גבוהה לכלול בין השאר את הנושאים האלה:

---

47 לפי סעיף 3 לחוק (תיקון 13 לחוק שייכנס לתוקף ב-14.8.25). יצוין כי קודם התיקון לחוק הוגדרה אבטחת מידע כהגנה על שלמות המידע או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכול בלא רשות כדין (סעיף 7 לחוק).

48 לפי תקנה 4 לתקנות.

49 לפי תקנה 4(ד)3 לתקנות.

50 לפי תקנה 3(2) לתקנות.

תרשים 17: **נושאים עיקריים שיש לכלול בנוהל אבטחת מידע למאגרים ברמת אבטחה בינונית וגבוהה**

לפי תקנות אבטחת מידע, בעיבוד משרד מבקר המדינה.

ארגון שהוא בעל שליטה בכמה מאגרי מידע רשאי לקבוע נוהל אבטחה במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה. כמו כן, על בעל השליטה במאגר לבחון את הצורך בעדכון הנוהל אחת לשנה לפחות[51].

באוקטובר 2024, במסגרת מינוי הממונה על אבטחת מידע במאגרי המידע של משרד הביטחון, הגדיר ראש אגף התקשוב כי אחד מתפקידי הממונה שכפופה אליו הוא להכין נוהל אבטחה ארגוני שמטרתו לייצר מדיניות אבטחה להתמודדות עם סיכוני האבטחה שלהם חשוף המידע; זאת בהתאם לנדרש בתקנות. לבקשת משרד מבקר המדינה לקבל נוהל אבטחה ארגוני שכולל הוראות אבטחה פיזית, הרשאות גישה, תיאור אמצעי אבטחה והתמודדות עם אירועי אבטחה, הפנה אגף התקשוב את משרד מבקר המדינה לאגף ביטחון.

אגף ביטחון קבע נהלים שונים הנוגעים לאבטחת מידע בנכסי התקשוב של משרד הביטחון; בחלקם קיים מענה לנושאים שאותם יש לכלול בנוהל האבטחה של מאגרי מידע ברמת אבטחה בינונית וגבוהה, דוגמת ניהול אירועי סייבר, מדיניות סיסמאות שהיא חלק ממדיניות הגישה למאגרים והגנה בעבודה עם התקנים ניידים. כמו כן, בנהלים מסוימים אגף ביטחון נותן את דעתו לסוגיית הגנת הפרטיות. למשל, בהנחייתו בנוגע לשימוש בטכנולוגיות המתקדמות של בינה מלאכותית (AI)[52] ניתנו לעובדי משרד הביטחון כלים לאבטחת מידע ולהגנת הפרטיות בעת שימוש במודל שפה ציבורי וכן ניתנה הנחיה לקציני הביטחון שבמשרד לבצע הדרכה לעובדים על נוהלי אבטחת מידע והגנה על הפרטיות לפני תחילת השימוש במודל שפה. לדברי ראש אגף ביטחון, כפי שנמסרו למשרד מבקר המדינה בינואר 2025, אגף ביטחון הוא האחראי להגדרת התקינה, הנהלים, תפיסות ההגנה ואבטחת המידע, והידע הנדרש לכך מצוי ביחידות המקצועיות של האגף; ואילו אגף התקשוב מונחה על ידי אגף ביטחון ונדרש לממש את הנחייתו בכלל היבטי הביטחון וההגנה.

על אף האמור, בפגישה שקיימו נציגי משרד מבקר המדינה עם נציגי אגף ביטחון בספטמבר 2024 נמסר כי לא קיים נוהל מסוים שנוגע לאבטחת מידע מתוקף חוק הגנת הפרטיות, ונוהל כזה לא נמסר למשרד מבקר המדינה עד למועד סיום הביקורת, ינואר 2025. כמו כן, משרד הביטחון קבע בהוראותיו הוראה בנושא אבטחת מידע ורשומות שמתייחסת לאמצעים שונים למידור ולאבטחה שנועדו להבטיח כי מידע בכלל, וזה הכלול ברשומות בפרט, יגיע רק אל מי

51 לפי תקנה 4(ה) לתקנות.

52 הנחיות הגנה לשימוש במודל שפה (בינה מלאכותית) לטובת שליפת מידע, 20.8.24.

שצריך להיחשף אליו ומורשה לכך. אולם, הוראה זו עוסקת באבטחת מידע בהיבט הביטחוני של מידע מסווג ואינה עוסקת בהיבטים של הגנת הפרטיות.

בביקורת עלה כי אגף התקשוב לא קבע נוהל אבטחה למאגרי המידע בהתאם לנושאים הנדרשים בתקנות. נושאים מסוימים שאותם יש לכלול בנוהל קיימים בנהלים שקבע אגף ביטחון, דוגמת ניהול אירועי סייבר, הגנה בעבודה עם התקנים ניידים ומדיניות סיסמאות, שהיא חלק ממדיניות הגישה למאגרים; אולם נושאים כגון הסיכונים שלהם חשופים מאגרי המידע, אופן קביעת הסיכונים והטיפול בהם ואופן הבקרה על השימוש במאגרים, אינם מקבלים מענה בנהלים מצד אף גורם במשרד הביטחון.

בהיעדר נוהל אבטחה למאגרי המידע נותר משרד הביטחון בלא מדיניות אבטחה סדורה ושלמה להתמודדות עם סיכוני האבטחה שלהם חשוף המידע שבמאגרי מידע ובלא כלי לעריכת ביקורות תקופתיות שיאפשרו לו לוודא את קיומם של אמצעי האבטחה הנדרשים לפי הנוהל ואת תקינותם.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-קביעת נוהל אבטחה למאגרי המידע בסכום שבין 40,000 ש"ח למאגר ברמת אבטחה בינונית ל-160,000 ש"ח למאגר ברמת אבטחה גבוהה.

על מנכ"ל משרד הביטחון לוודא כי ייקבע נוהל אבטחה משרדי למאגרי המידע כנדרש בתקנות שיבטיח את יישום מדיניות האבטחה הנדרשת בהיבטי הגנת הפרטיות וכן את אופן הטיפול בסיכונים ובאירועי אבטחה.

2. סקרי סיכונים ומבדקי חדירות

בעל שליטה במאגר מידע שחלה עליו רמת אבטחה גבוהה נדרש לביצוע סקר לאיתור סיכוני אבטחת מידע אחת ל-18 חודשים לפחות. עם סיום הסקר וגיבוש ממצאיו עליו לדון בממצאי הסקר ולבחון את הצורך בעדכון מסמך הגדרות המאגר או בעדכון נוהל האבטחה של מאגר המידע ולפעול לתיקון ליקויים בתחום האבטחה, אם התגלו[53]. כמו כן, בעל שליטה במאגר מידע שחלה עליו רמת אבטחה גבוהה אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים אחת ל-18 חודשים לפחות, ועליו לדון בתוצאות מבדקי החדירות ולפעול לתיקון הליקויים שהתגלו, אם התגלו[54]. ארגון שהוא בעל כמה מאגרי מידע רשאי לקיים סקר סיכונים אחד ומבדק חדירות אחד לכל מאגרי המידע שברשותו המצויים באותה רמת האבטחה, זאת אחת ל-18 חודשים לפחות.

מטרתו של סקר הסיכונים היא להעריך את רמת הבשלות הארגונית להתמודדות עם איום לפגיעה בשלמות המידע בארגון, בסודיות שלו ובזמינותו, והוא משמש לקביעת סדרי העדיפויות לטיפול בסיכונים אלו ולהבנת הבקרות שעל הארגון ליישם בתוכניות העבודה שלו. מטרתו של מבדק חדירות היא לזהות את נקודות החולשה באבטחת המידע הארגונית כדי לבחון את יעילות הבקרות ומנגנוני ההגנה הקיימים[55].

בפגישה שקיימו נציגי משרד מבקר המדינה בספטמבר 2024 עם ראש היחידה למערכות מחשוב ליתרון הגנתי בסייבר באגף התקשוב היא מסרה כי אגף ביטחון אחראי לבצע סקרי סיכונים ומבדקי חדירות; וכן כי גם אגף התקשוב מבצע סקרי סיכונים ומבדקי חדירות לפי הצורך

---

53 לפי תקנה 5(ג) לתקנות.

54 לפי תקנה 5(ד) לתקנות.

55 לפי נייר עמדה של הרשות להגנת הפרטיות בנושא ביצוע סקר סיכונים ומבדק חדירות למערכות מידע, מאי 2024.

ובתדירות משתנה באמצעות היחידה שהיא עומדת בראשה. למשל, היחידה ביצעה סקר סיכונים על אתר אינטרנט שפיתחה חברה במיקור חוץ עבור האגף כדי לוודא כי אין חולשות באתר; כמו כן היחידה ביצעה מבדק חדירות על תהליך ההכרה הממוחשב באתר האינטרנט של אגף שיקום נכים[56]. עוד היא מסרה כי אגף התקשוב אינו מבצע סקרי סיכונים ומבדקי חדירות ייעודיים בנוגע למערכות מאגרי המידע ולמאגרים עצמם. בפגישה נוספת שהתקיימה עימה בנובמבר 2024, לאחר שמונתה לממונה על אבטחת מידע במאגרי המידע והוטל עליה בין היתר לבצע סקרי סיכונים תקופתיים, היא מסרה כי חברת הייעוץ שתייעץ לה בנושא הגנת הפרטיות תבצע סקרי סיכונים ומבדקי חדירות.

לדברי ראש אגף ביטחון מינואר 2025, אגף ביטחון נושא באחריות הכוללת להגנה, למניעה ולסיכול של תקיפות סייבר על כלל הנכסים הטכנולוגיים של משרד הביטחון. כמו כן הוא מופקד על אבטחת המידע ועל חשיפת מידע ביטחוני של משרד הביטחון בכל ממד שבו משתמש המשרד, ועל ביצוע בקרות, סקרי חוסן, תרגילי חדירה ועוד. בכך הוא מייצר תמונה מקצועית בלתי תלויה מתוקף אחריותו על פי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, ומתוקף היותו גורם מקצועי המופקד על ההגנה. כל זאת בשונה מאגף התקשוב, שהוא גורם תפעולי שמופקד על קידום תהליכים והוא אינו מוסמך לקבוע את מדיניות ההגנה, אבטחת המידע, התקינה ואופן ניהול הסיכונים, ואין לו את הידע הנדרש ואת ההכשרות הנדרשות בתחום ניהול הסיכונים. אולם, לדבריו, נכון שאגף התקשוב יפעיל בקרות עצמיות כדי לוודא שהוא עומד בדרישות אגף ביטחון[57]. עוד מסרו נציגי אגף ביטחון בספטמבר 2024 כי האגף מבצע סקרי סיכונים ומבדקי חדירות בהתאם להנחיות של מלמ"ב[58] וכן מנטר את רשתות המחשב במשרד הביטחון באמצעות מרכז הבקרה להגנת סייבר (SOC)[59] כך שתוקֵף צריך לעבור את מרכיבי ההגנה כדי להגיע למאגרי המידע.

לבקשת משרד מבקר המדינה העביר לו אגף ביטחון סקרי סיכונים ומבדקי חדירות שהוא ביצע בשלוש השנים האחרונות, ומהם עלה כי בוצעו מבדקי חוסן לרשתות מחשבים וסקרי אבטחה למערכות מידע שונות במשרד הביטחון. אולם, סקרי סיכונים ומבדקי חדירות אלו לא נעשו בהתייחס למאגרי המידע - הם לא זיהו, לא ניתחו ולא העריכו את התרחישים האפשריים להתרחשות אירוע אבטחה במאגרים באופן פרטני או בשלבי התהליך העסקי שנוגע אליהם, ואת סבירותם להתממש; הם לא התבססו על מיפוי מאפייני מערכות המידע המעבדות מידע מהמאגרים, לרבות אמצעי האבטחה להגנתן; והם לא כללו מיפוי של הפעולות והבקרות הקיימות בארגון, למול הפעולות והבקרות שראוי ליישם לצורך מזעור סבירות התממשות הסיכונים.

בביקורת עלה כי אגף התקשוב לא ביצע סקרים לאיתור סיכוני אבטחת מידע במאגרי המידע שהם ברמת אבטחה גבוהה ולא ערך מבדקי חדירות למערכות של המאגרים האלה לצורך בחינת עמידותן בפני סיכונים פנימיים וחיצוניים, כפי שנדרש בתקנות הגנת הפרטיות (אבטחת מידע). אגף התקשוב ואגף ביטחון מבצעים סקרי סיכונים ומבדקי חדירות ברשתות ובמערכות מידע שונות במשרד הביטחון ובאתרי אינטרנט של משרד הביטחון שמפתחות

---

56 צוין כי אין גישה מאתר האינטרנט של אגף שיקום נכים למאגר המידע של נכי צה"ל, ולא ניתן לדלות מהאתר פרטים על נכי צה"ל.

57 עוד ציין ראש אגף ביטחון כי גם בסוגיית אבטחת מידע בחברות חיצוניות שיש להן גישה למערכות המחשב ולמאגרי המידע של משרד הביטחון, כגון חברות פיתוח, האגף פועל להגן על המידע של משרד הביטחון באמצעות וידוא עמידה ביישום תקן רב-מגן 2.0 של מלמ"ב, שהוא תקן הגנה בסייבר למידע ביטחוני, המותאם לתקינה אזרחית בין-לאומית. ובאופן כללי, מלמ"ב מנחה את האגף בנוגע לתקינה שחלה עליו, ויש תקנים כגון תקן אבטחת מידע ארגוני ISO27001 שאותו הוא לא נדרש ליישם.

58 למשל, הוא פועל על פי תקן אבטחת רשתות ותשתיות מחשב של מלמ"ב מינואר 2023, הכולל התייחסות לסיכונים הביטחוניים השכיחים דוגמת ניצול הרכיבים הטכנולוגיים של רשת ותשתית מחשוב, תהליכיה ומשתמשיה על ידי גורמים עוינים לטובת גניבת סודות, יצירת שיבושים, נזק או ביצוע מניפולציות שונות, וכן כולל את דרישות הביטחון הנדרשות לסגירת פערים אלו, ויש בו תאימות מול תקינה בינלאומית.

59 Security Operation Center - יחידה בארגון האחראית לתהליכים ולטכנולוגיה ונועדה לפקח באופן רציף על רמת האבטחה של הארגון ולשפר אותה, תוך ביצוע פעולות מניעה, ניתוח, ותגובה לגבי אירוע אבטחת רשת. יצוין כי ה-SOC של משרד הביטחון אינו מחובר ל-SOC הממשלתי.

חברות במיקור חוץ כדי לוודא שאין בהם חולשות אבטחה; אולם, אף גורם במשרד הביטחון לא ביצע סקרי סיכונים ומבדקי חדירות ייעודיים בנוגע ל-14 מאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם - הוא לא זיהה, לא ניתח ולא העריך את התרחישים האפשריים להתממשות אירוע אבטחה במאגרים באופן פרטני או בשלבי התהליך העסקי שנוגע אליהם ואת סבירותם להתממש; הוא לא התבסס על מיפוי מאפייני מערכות המידע המעבדות מידע מהמאגרים; והוא לא כלל מיפוי של הבקרות הקיימות בארגון למול הבקרות שראוי ליישם למזעור הסבירות להתממשות הסיכונים. ממילא משרד הביטחון לא בחן את הצורך בעדכון מסמך הגדרות המאגר או בעדכון נוהל אבטחה למאגרי מידע; הוא לא קבע את הבקרות הנדרשות; ולא בחן את יעילות הבקרות ומנגנוני ההגנה הקיימים.

בהיעדר סקרי סיכונים ומבדקי חדירות למאגרי המידע אין למשרד הביטחון את הכלים להעריך את רמת הבשלות שלו להתמודדות עם איום לפגיעה בשלמות המידע האגור במאגרי המידע, בסודיות שלו ובזמינותו; לזהות את נקודות החולשה באבטחת המידע; לקבוע סדרי עדיפויות לטיפול בסיכונים אלו; להבין את הבקרות שעליו ליישם בתוכניות העבודה שלו; ולבחון את יעילות הבקרות ואת מנגנוני ההגנה הקיימים.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-ביצוע סקרי סיכונים ומבדקי חדירות כפי שנדרש בתקנות בסכום של 320,000 ש"ח.

על משרד הביטחון לבצע סקרים לאיתור סיכוני אבטחת מידע במאגרי המידע שהם ברמת אבטחה גבוהה ולערוך מבדקי חדירות למערכות של המאגרים האלה לצורך בחינת עמידותן בפני סיכונים פנימיים וחיצוניים, כפי שנדרש בתקנות.

3. הדרכת העובדים והגברת מודעותם

בעל שליטה במאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה נדרש לקיים פעילות הדרכה תקופתית לבעלי הרשאות למאגר בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע המצוינות בחוק ובתקנות, זאת בהיקף הנדרש לביצוע תפקידיהם. כמו כן, על ההדרכה לעסוק בחובות של בעלי ההרשאות לפי נוהל האבטחה, החוק והתקנות. יש לבצע את ההדרכה אחת לשנתיים לפחות[60]. גם הוראת משרד הביטחון בנושא אבטחת מידע ורשומות[61] קובעת כי אחד העקרונות לאבטחת רשומות הוא הדרכת העובדים העוסקים בהן.

אגף התקשוב מבצע פעולות שונות להגברת המודעות של העובדים בנוגע להגנת הפרטיות, כגון הודעת תזכורת בשומר המסך ברשת התקשורת הבלתי מסווגת של משרד הביטחון והפצת תזכורות לראשי האגפים במשרד הביטחון אחת לשנה לבצע "בדק בית" באגף בנוגע להעברת מידע מתוך מאגרי המידע. נוסף על כך, קיימת בפורטן הארגוני של משרד הביטחון תחת עמוד האינטרנט של אגף התקשוב לומדה אינטראקטיבית בנוגע להגנת הפרטיות. לדברי אגף התקשוב, כפי שנמסרו למשרד מבקר המדינה בדצמבר 2024, הלומדה אינה נשלחת למשתמשים באופן יזום, כפי שמבוצע לדוגמה בלומדה למניעת הטרדה מינית במשרד הביטחון; משתמשים המעוניינים לגשת ללומדה נכנסים לעמוד האינטרנט של אגף התקשוב בפורטן הארגוני ומפעילים אותה ביוזמתם. כמו כן, אין לאגף התקשוב כלי לרישום הנכנסים ללומדה אך בכוונת האגף להוסיף כלי לבקרה אחר הנכנסים ללומדה בשנת 2025.

גם אגף ביטחון מבצע פעולות שונות להגברת המודעות לאיומי סייבר ואבטחת מידע, לרבות תוכנית הסברתית ביטחונית לכלל העובדים והמשרתים במשרד הביטחון בכל תחומי הביטחון בשיתוף עם אגף דוברות וקשרי ציבור במשרד הביטחון, בדגש על היכרות עם איומי הסייבר

60 לפי תקנה 7(ג) לתקנות.

61 הוראת משרד הביטחון מס' 14.02.

השונים ודרכי ההתגוננות מפניהם; קיום תרגילים להגברת המודעות לאיומי סייבר, דוגמת תרגילי דיוג (פישינג) שממצאיהם הוצגו בפורום הנהלת המשרד; והפצת מסמך לעובדים בנושא הגברת המודעות לאיומי סייבר בשימוש בכלי בינה מלאכותית (AI) בחשבונות אישיים (כגון אי-מסירת מידע על מקום עבודתו או פרטים שעלולים לחשוף זאת). אולם, אגף ביטחון מסר למשרד מבקר המדינה בספטמבר 2024 כי ההדרכות בתחומי הגנת הפרטיות הן באחריות אגף התקשוב.

בביקורת עלה כי אגף התקשוב אינו מבצע אחת לשנתיים לפחות פעילות הדרכה לבעלי ההרשאות למאגרי המידע שברמת אבטחה בינונית או גבוהה בהתאם לנדרש בתקנות. אגף התקשוב מבצע פעולות להגברת המודעות בנוגע להגנה על הפרטיות, כגון תזכורות בשומר המסך של המשתמשים במערכות המחשוב וחידוד הנהלים בנוגע להעברת מידע ממאגרי המידע, ואגף ביטחון מבצע פעולות שונות להגברת המודעות לאיומי סייבר ואבטחת מידע; אולם אף גורם במשרד הביטחון אינו מקיים פעילויות הדרכה אחת לשנתיים לפחות בדבר הוראות אבטחת המידע המצוינות בחוק ובתקנות, וגם לא בדבר מסמכי הגדרות המאגרים ונוהל האבטחה של המאגרים, שממילא אינם קיימים ברשות משרד הביטחון באופן סדור.

מצב שבו משתמשים בעלי הרשאות למאגרי המידע של משרד הביטחון אינם מתודרכים באופן סדור בנוגע לחשיבות אבטחת המידע שאליו הם נחשפים בהיבטי הגנת הפרטיות ובנוגע לפעולות שעליהם לנקוט לצורך שמירה על המידע, עלול להוביל לביצוע פעולות שאינן בהתאם להנחיות הנוגעות לשמירה על המידע הקיים במאגרים.

עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-קיום הדרכות אחת לשנתיים לפחות לבעלי הרשאות למאגרי המידע כנדרש בתקנות בסכום שבין 20,000 ש"ח למאגר ברמת אבטחה בינונית ל-80,000 ש"ח למאגר ברמת אבטחה גבוהה.

עוד עלה בביקורת כי אף שאגף התקשוב פיתח לומדה אינטראקטיבית בנושא הגנת הפרטיות במסגרת הדרישות החלות עליו להגברת המודעות של העובדים לנושא, הוא אינו מבצע בקרה על בעלי התפקידים שנכנסו ללומדה משום שהכניסה ללומדה היא ביוזמתם, ואין לאגף כלי לרישום הנכנסים. כתוצאה מכך פוחתת האפקטיביות של הלומדה ככלי להגברת מודעות העובדים.

על משרד הביטחון לבצע פעילות הדרכה אחת לשנתיים לפחות לבעלי ההרשאות למאגרי המידע שברמת אבטחה בינונית או גבוהה בהתאם לנדרש בתקנות.

כמו כן, מומלץ כי אגף התקשוב יפיץ לבעלי התפקידים הרלוונטיים את הלומדה האינטראקטיבית בנושא הגנת הפרטיות, יוודא כי הם נכנסים אליה באמצעות כלי לרישום הנכנסים ויבצע על כך בקרה ומעקב.

☆

מהאמור לעיל עלה כי אגף התקשוב לא מימש את האחריות שהוא נושא בה לקיים את הדרישות החלות על משרד הביטחון בתחום אבטחת המידע במאגרי המידע בהיבטי הגנת הפרטיות, ובהן קביעת נוהל אבטחה וביצוע סקרי סיכונים, מבדקי חדירות והדרכה להגברת המודעות של העובדים; זאת משום שהוא נסמך על אגף ביטחון, שהוא הגורם המקצועי ובעל הסמכות בתחום אבטחת המידע של משרד הביטחון, בלא שווידא כי הפעולות שאגף ביטחון מבצע אכן נותנות מענה לכלל הדרישות הייחודיות בהיבט הגנת הפרטיות. יצוין כי אגף ביטחון מבצע פעולות לאבטחת מידע, אולם פעולות אלה דרושות לשם שמירה על מידע מסווג כהגדרתן בחוק להסדרת

הביטחון בגופים ציבוריים, התשנ"ח-1998, שמכוחו פועל האגף[62], והן לא נותנות מענה מלא לאבטחת המידע במאגרי המידע בהיבט הגנת הפרטיות.

אי-עמידה בדרישות אבטחת המידע מתוקף תקנות הגנת הפרטיות מגבירה את הסיכונים הנשקפים למאגרי המידע, ובהם דֶלֶף מידע, שיבוש מידע או פגיעה בזמינותו, זאת בפרט נוכח האתגרים הייחודיים הקיימים באכיפה הנוגעת להגנת הפרטיות במאגרי מידע ממוחשבים. בשנים האחרונות דֶלֶף מידע מתוך משרד הביטחון הן כתוצאה מתקיפות סייבר מצד גורמים חיצוניים עוינים שהדליפו מידע מתוך פורטלים מינהליים של משרד הביטחון, לרבות מידע מזהה של עובדי המשרד, מידע על מכרזים ביטחוניים ומידע על מערכות טכנולוגיות של צה"ל, ובכלל זה תשריטים הנדסיים ומידע טכני; והן כתוצאה מטעויות אנוש של עובדים שפרסמו בשגגה מספרי תעודות זהות, שמות ומספרי רכב של בכירים במשרד הביטחון.

מומלץ כי מנכ"ל משרד הביטחון יסדיר את תחומי האחריות והסמכות בתחום אבטחת המידע במאגרי המידע מתוקף חוק הגנת הפרטיות ותקנות אבטחת מידע, לדוגמה באמצעות מינוי גורם אחד שיישא באחריות הכוללת ויהיה בעל ראייה מתכללת בנוגע לכלל היבטי אבטחת המידע, לרבות בראי הגנת הפרטיות; באמצעות הקמת צוות בין-אגפי לחיזוק אבטחת המידע במאגרי המידע, שיכלול למשל נציגים מאגף ביטחון, מאגף התקשוב, מאגף היועץ המשפטי למערכת הביטחון ומאגפים שמשתמשים במאגרי המידע; או בכל דרך אחרת שימצא לנכון. עוד מומלץ כי חלוקת האחריות, הסמכות והתפקידים השונים, לרבות בהתייחס לתיקון 13 לחוק הגנת הפרטיות, יעוגנו בנוהל משרדי.

בתגובתו ממאי 2025 על ממצאי הביקורת ציין משרד הביטחון כי הוא רואה חשיבות רבה בהגנה על מאגרי המידע שבאחריותו ובחיזוק מתמיד של אמצעי אבטחת המידע והגנת הפרטיות; זאת כחלק בלתי נפרד ממחויבותו לשמירה על הביטחון ולהגנה על נכסי המשרד ועל מרכיבי הרציפות התפקודית החיונית, מתוך הבנה כי מידע אישי ורשומות ממוחשבות הם כיום רכיב רגיש וחיוני "ממש כמו תשתיות פיזיות". עוד ציין משרד הביטחון כי נכון למועד הביקורת היו פערים שנבעו מהאצת תהליכים טכנולוגיים, וכי במסגרת בחינה מעמיקה של הסוגיות שעלו בדוח זה המשרד מקיים דיונים עם הרשות להגנת הפרטיות ועם כלל הגורמים הרלוונטיים במשרד - אגף התקשוב, אגף הביטחון, היועץ המשפטי למערכת הביטחון ואגף התכנון - במטרה לקבוע מהן החלופות הטובות והמתאימות ביותר להסדרת הנושא באופן המיטבי. כמו כן הוא פועל באינטנסיביות לגישור על הפערים ולהשלמת היערכותו למתן מענה מקיף ועדכני שיעמוד בדרישות החוקיות והמקצועיות ברמה הגבוהה ביותר. עוד ציין משרד הביטחון כי דוח ביקורת זה משמש עבורו כלי אפקטיבי שתורם להכוונת פעולות המשרד לקידום פעולות ההסדרה, בייחוד לנוכח מועד הביקורת - ערב כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות.

<u>הרשות להגנת הפרטיות</u>

הרשות להגנת הפרטיות היא הגוף המאסדר של כלל המשק בתחום ההגנה על הזכות לפרטיות לרבות באמצעות פיקוח ואכיפה מינהלית ופלילית בנוגע לכלל מאגרי המידע האישי בישראל, בגופים פרטיים וציבוריים כאחד, המחזיקים או מעבדים מידע אישי דיגיטלי, זאת בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. נוכח מספרם הרב של הגופים המפוקחים על ידי הרשות ומגבלת המשאבים שלה, היא קובעת את תוכניות האכיפה והפיקוח שלה באמצעות ניהול סיכונים ותיעדוף, למשל על ידי מתן עדיפות לטיפול בגופים שמחזיקים במידע רגיש בהיקף נרחב ומתן קדימות לנושאים רגישים וכן על פי מידת ההשפעה הרוחבית של פעילות האכיפה.

---

62 אגף ביטחון נושא באחריות הכוללת להגנה, למניעה ולסיכול של תקיפות סייבר על כלל הנכסים הטכנולוגיים של משרד הביטחון; אחראי להגדרת התקינה, הנהלים, תפיסות ההגנה ואבטחת המידע; מופקד על ביצוע בקרות וסקרי חוסן; ועוד.

בפגישה שקיימו נציגי משרד מבקר המדינה בספטמבר 2024 עם נציגי הרשות להגנת הפרטיות, ובהם ראשת מטה הרשות להגנת הפרטיות, מנהל מחלקת ייעוץ משפטי ואסדרה, הממונה על הגנה מגזרית ומנהלת האכיפה המינהלית, נמסר כי הרשות להגנת הפרטיות לא ביצעה ביקורות ופעולות פיקוח על מאגרי המידע של משרד הביטחון.

כאמור, עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות באוגוסט 2025 יידרש משרד הביטחון למנות מפקח פרטיות בהתייעצות עם ראש הרשות להגנת הפרטיות ובהתאם לתנאי הכשירות וההכשרה שיורה עליהם ראש הרשות. מפקח הפרטיות יהיה כפוף ישירות למנכ"ל משרד הביטחון או למי מטעמו ויונחה מקצועית על ידי הרשות להגנת הפרטיות ובין היתר יידרש להגיש למנכ"ל משרד הביטחון ולראש הרשות דין וחשבון שנתי על קיום הוראות הדין בתחום הפרטיות במשרד הביטחון.

בתגובתה ממרץ 2025 על ממצאי הביקורת מסרה הרשות להגנת הפרטיות כי במסגרת היערכותה לכניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, היא שלחה מכתבים לראשי הגופים הביטחוניים, יזמה פגישות עבודה עימם שמטרתן לדון על סדרי עבודה ונוהלי העבודה בין הגופים, וציינה את תנאי הכשירות וההכשרה המתאימים לדעתה בכל גוף וגוף, ובכלל זה במשרד הביטחון.

נמצא כי הרשות להגנת הפרטיות מעולם לא ביצעה ביקורות ופעולות פיקוח על משרד הביטחון ואף לא ביקשה ממשרד הביטחון דיווחים בנוגע לבקרות שהוא ביצע על יישום הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.

בדוח ביקורת זה עלו ליקויים בנוגע לאופן שבו משרד הביטחון מנהל את מאגרי המידע שהוא בעל השליטה בהם ואת אבטחתם, ובכלל זה בנוגע למיפוי ורישום המאגרים, לסיווגם, לביצוע סקרי סיכונים ומבדקי חדירות, לניהול הרשאות הגישה למאגרי המידע ולביצוע בקרה על יישום כלל הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.

לנוכח זאת, מומלץ כי הרשות להגנת הפרטיות, שהיא הגורם המאסדר גם לעניין גופים ביטחוניים, תפקח על האופן שבו משרד הביטחון מיישם את הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, בשימת לב לליקויים שצוינו בדוח ביקורת זה. כמו כן, מומלץ כי הרשות תיתן למפקח הפרטיות האמור הנחיות מקצועיות בהתאם לסמכויותיה על פי תיקון 13 לחוק הגנת הפרטיות, בדגש על הסוגיות שבהן פעילותו של משרד הביטחון לוקה בחסר.

סיכום

משרד הביטחון הוא בעל שליטה במאגרים הכוללים מידע אישי, כגון נתונים על אישיותו של אדם, מצבו הבריאותי ומצבו הכלכלי. הסיכונים להגנת הפרטיות ולאבטחת המידע שבמאגרים אלו התגברו לנוכח מלחמת חרבות ברזל והתממשותם עלולה לפגוע ביכולתו של משרד הביטחון לספק את האמצעים הנדרשים לצה"ל, לגרום לו נזק תדמיתי, לפגוע ביחסיו עם ספקים ולקוחות ולחשוף אותו לקנסות. יתרה מכך, הדבר אף עלול לזרוע בהלה ותחושת חוסר ביטחון בציבור ולפגוע בקשרי החוץ של המדינה בהקשרים ביטחוניים-מדיניים.

בשנים האחרונות דָלַף מידע מתוך משרד הביטחון הן כתוצאה מתקיפות סייבר מצד גורמים חיצוניים עוינים והן כתוצאה מטעויות אנוש של עובדי המשרד, לרבות מידע מזהה על בעלי תפקידים במשרד הביטחון.

תמונת המצב העולה מדוח זה מצביעה על פערים חמורים באופן שבו משרד הביטחון מנהל את 14 מאגרי המידע שהוא בעל השליטה בהם ואת אבטחתם, ושבהם קיימים נתונים אישיים בנוגע ל-2.84 מיליון איש. בביקורת עלה כי אגף התקשוב, הנושא באחריות לקיים את הדרישות החלות על משרד הביטחון מתוקף חוק הגנת הפרטיות ותקנות אבטחת מידע, לא מיפה את כלל המאגרים

שבבעלות משרד הביטחון משנת 2007, הוא לא קבע נוהל אבטחה למאגרי המידע, לא ביצע סקרים לאיתור סיכוני אבטחת מידע במאגרי המידע שהם ברמת אבטחה גבוהה ולא ערך מבדקי חדירות למערכות של המאגרים האלה לצורך בחינת עמידותן בפני סיכונים פנימיים וחיצוניים.

נוסף על כך, בדוח עלו ליקויים בנוגע לניהול הרשאות המשתמשים במערכת ניהול זהויות ובמערכת המידע המקושרת למאגר נכי צה"ל - מאגר שבו אגור מידע על אודות כ-230,000 אנשים ובהם גם כ-18,000 פצועים שנוספו אליו בשל מלחמת חרבות ברזל, לרבות מידע על מצבם הבריאותי, מצבם הכלכלי, בני משפחותיהם והשירותים הניתנים להם. מניתוח שביצע משרד מבקר המדינה עלה כי 5 מכל 10 משתמשים חיצוניים (עובדי מיקור חוץ) בעלי הרשאת גישה פעילה למערכת המידע המקושרת למאגר נכי צה"ל, לא נכנסו אליה יותר מחצי שנה. גם יועצים, שמנוהלים במערכות כוח האדם של משרד הביטחון בדומה לעובדי המשרד, לא נכנסו למערכת יותר מחצי שנה, ושיעורם מסך כל המשתמשים שלא נכנסו למערכת היה 20%. במצב זה עולה החשש כי הם בעלי הרשאות למאגר נכי צה"ל שלא לצורך.

על משרד הביטחון לעמוד בדרישות החלות עליו בהיבטי הגנת הפרטיות כמתחייב בחוק ובתקנות, ובפרט לאור תיקון 13 לחוק, שייכנס לתוקף באוגוסט 2025, המתאים את החוק לאתגרים העכשוויים. כמו כן, נוכח הממצאים שעלו בניתוח הנתונים שביצע משרד מבקר המדינה, מומלץ כי משרד הביטחון יבדוק את תהליכי ניהול ההרשאות בכלל מערכות המידע שמקושרות למאגרי המידע של משרד הביטחון. עוד מומלץ כי מנכ"ל משרד הביטחון יסדיר את תחומי האחריות והסמכות בין אגף התקשוב ובין אגף ביטחון בתחום אבטחת המידע במאגרי המידע בראי הגנת הפרטיות. זאת, כדי לצמצם את הסיכונים לפגיעה בפרטיות ולפגיעה במימוש ייעודו של משרד הביטחון.