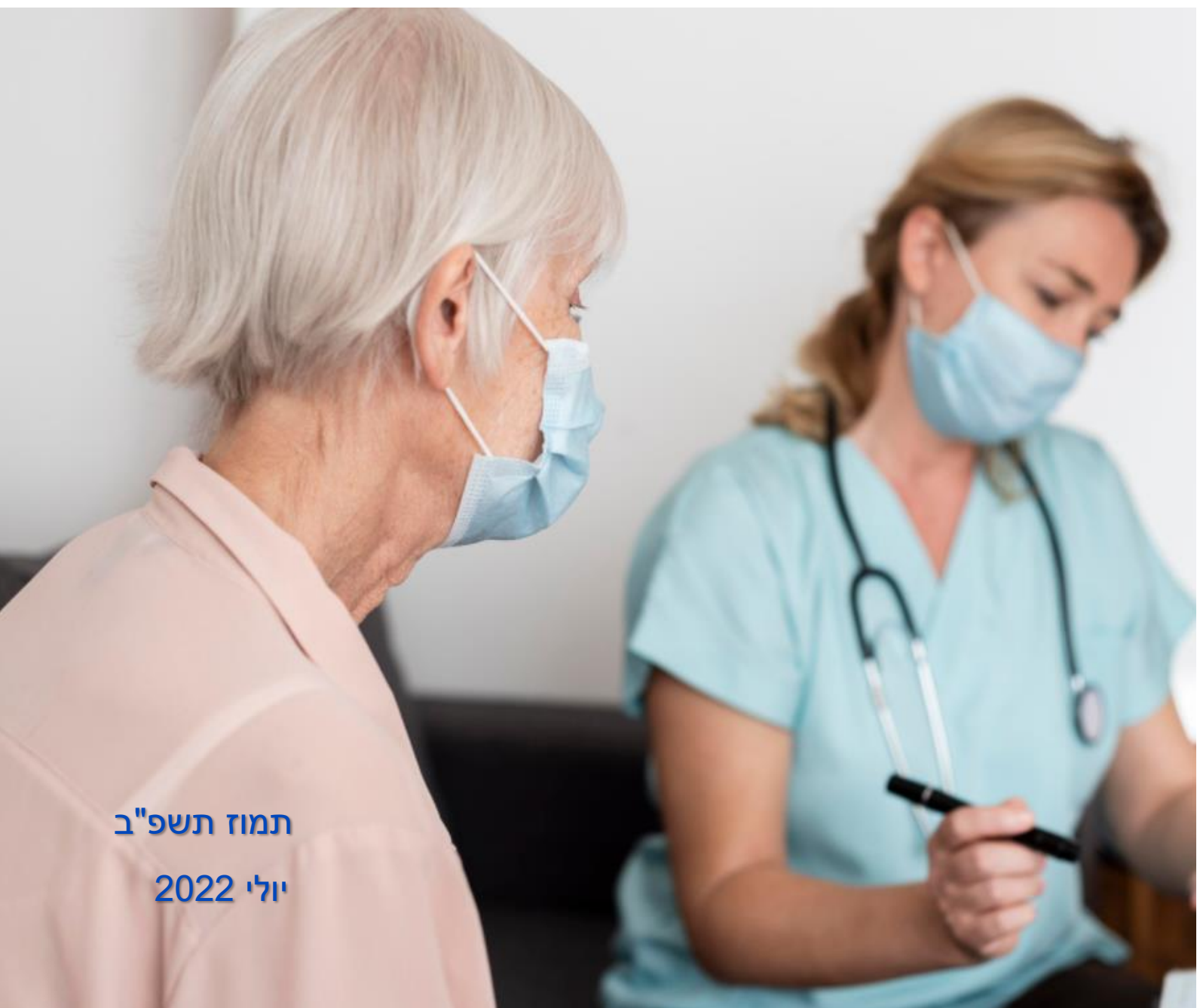




דוח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב חברות סיעוד



תמוז תשפ"ב

יולי 2022



1. תוכן עניינים

1.....	תוכן עניינים	1.
2.....	תקציר מנהלים	2.
2.....	מגזר חברות סיעוד	2.1
3.....	תהליך העבודה	2.2
4.....	ליקויים, מסקנות והמלצות עיקריות	2.3
8.....	מגזר חברות הסיעוד - תמונת מצב	3.
8.....	כללי	3.1
8.....	רקע על המגזר	3.2
10.....	תהליך העבודה	3.3
12.....	ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי	4.
13.....	בקרה ארגונית	4.1
14.....	ניהול מאגרי מידע	4.2
14.....	אבטחת מידע	4.3
15.....	עיבוד מידע אישי במיקור חוץ	4.4
16.....	מסקנות/תמונת מצב והמלצות	5.
16.....	בקרה ארגונית	5.1
16.....	ניהול מאגרי מידע	5.2
17.....	אבטחת מידע	5.3
17.....	עיבוד מידע אישי במיקור חוץ	5.4
18.....	שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב	6.
19.....	סיכום	7.
20.....	נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם	8.



2. תקציר מנהלים

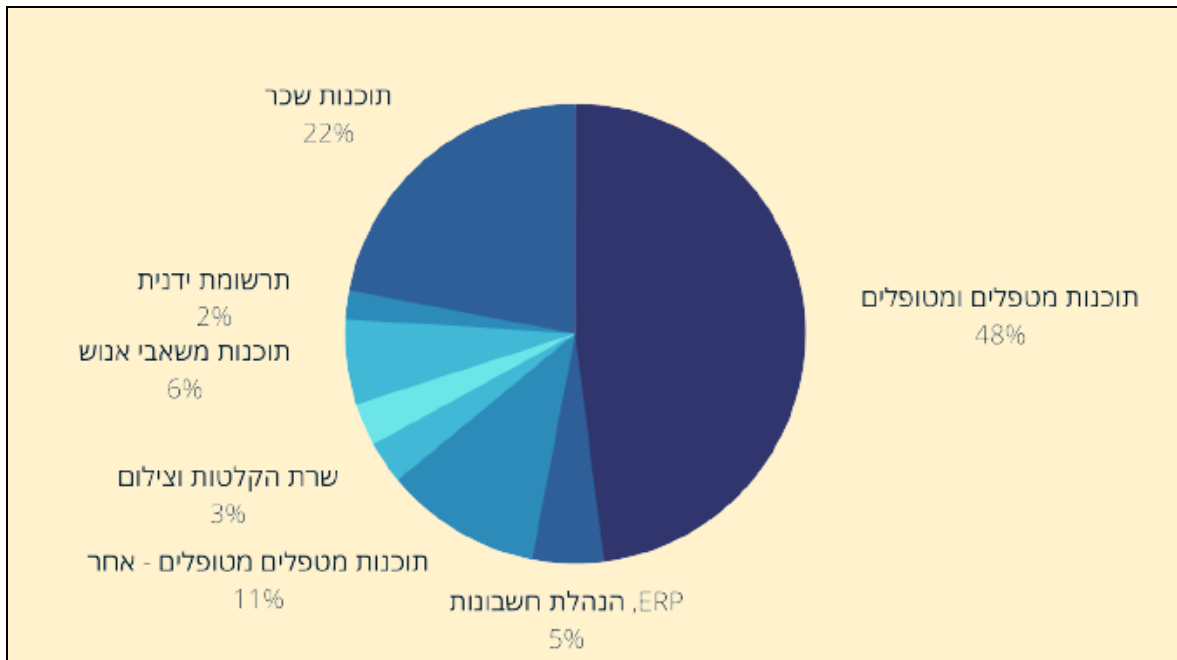
מערך פיקוח הרחוב ברשות להגנת הפרטיות, מופקד על עריכת פיקוחי רחוב מגזריים או נושאים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א-1981 ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. זאת, כדי לאתר הפרות של החוק והתקנות, לשם הגברת מודעות המשק להוראות החוק, להגברת האכיפה היוזמת של הרשות, לאתר כשלים ענפיים כלל-משקיים הדורשים התייחסות מוגברת של הרגולטור, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

2.1 מגזר חברות סיעוד

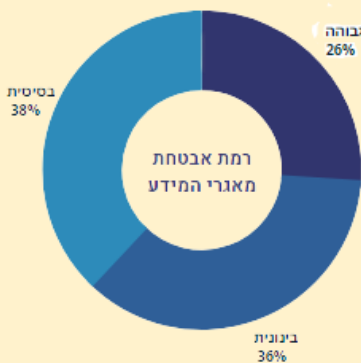
במסגרת סקר רחבי שערכה הרשות להגנת הפרטיות, שבחן את סיכוני הפרטיות במגזרים השונים במשק, מגזר חברות סיעוד אותר כאחד מיעדי פיקוח הרחוב המשמעותיים. מאגרי המידע של חברות הסיעוד כוללים מידע רפואי-סיעודי רגיש על מאות אלפי מטופלים, וכן אלו אלפי רשומות המכילות נתונים אישיים אודות מטופלים המועסקים דרך אותן חברות הסיעוד.

מגזר חברות הסיעוד הינו בעל מאפיינים ייחודיים בהיבטי פרטיות, הבאים לידי ביטוי, בין היתר, בהחזקת מידע רגיש על מצבם הבריאותי של לקוחות חברות הסיעוד; ריכוז מידע בריאותי וסיעודי ממספר גורמים מדווחים (מטופלים, בני משפחתם, המוסד לביטוח לאומי וכדו'); חברות הסיעוד שחלקן בעלות מספר סניפים ברחבי הארץ, משרתות אלפי לקוחות ומחזיקות במאגרי מידע בהיקפים עצומים; פערי כוחות משמעותיים בין בעלי המאגרים לבין המטופלים, הנובעים מהעובדה שלחלק מנושאי המידע תפקוד פיזי או קוגניטיבי נמוך, העלול להתאפיין גם במודעות נמוכה לפרטיות, לסיכונים הנובעים משימוש במידע עליהם, או לזכויות המוקנות להם.

ממצאי פיקוח הרחוב עולה כי חברות הסיעוד מנהלות ומחזיקות מגוון סוגים של מידע, כאשר למעלה ממחציתו הוא מידע על מטופלים, המנוהל לרוב על ידי שתי תוכנות מדף עיקריות. יתר המידע כלל מידע על עובדים ועובדות, תנאי שכר, מערכות לתכנון משאבי ארגוני (ERP) ובינה עסקית (BI) ואף מידע הכולל הקלטות וצילומים.



הגופים שנבחנו סווגו בהתאם לרמת אבטחת המידע, כפי שזו הוגדרה ופורטה בתוספת לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. מהפיקוח עלה כי מרבית הגופים שנבדקו במגזר



זה מנהלים מאגרי מידע ברמת אבטחת מידע בינונית או גבוהה (72%), והיתר מנהלים מאגרים ברמת אבטחה בסיסית (38%). רמת אבטחת המידע הנדרשת למאגרים מתפלגת בהתאם לגודל הגופים ומספר נושאי המידע, כאשר רמות העמידה הגבוהות נמצאו בגופים להם מאות משתמשים מורשי גישה למאגרים, ורמות העמידה הבינוניות והנמוכות נמצאו בגופים הבינוניים והקטנים להם מספר קטן יותר של מורשי גישה. בין יעדי הפיקוח

שנבדקו, נמצא כי צורת ההתאגדות השכיחה הינה חברה בע"מ (87% מהגופים שנבדקו), בעוד שיתר גופי הסיעוד שנבדקו מאוגדים כעמותות (13% מהגופים שנבדקו).

נוכח פערי הכוחות בין הצדדים, והמאפיינים שהוצגו לעיל, נדרשת מחברות הסיעוד הקפדה מיוחדת על עמידה בדרישות החוק, בדגש על זכויות נושאי המידע, מלרבות קיום רמת אבטחת מידע גבוהה, הדרכות שוטפות ובקרה שוטפת אחר המידע הרגיש במאגרים.

2.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרחב הרשות פנתה ל-40 גופים המנהלים חברות סיעוד בדרישה למילוי שאלוני ביקורת. נציין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע וכמות הלקוחות

וכן רגישות המידע במסגרת השירותים הניתנים ללקוחות. שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע, אבטחת מידע, ושימוש בשירותי מיקור חוץ. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. בהליך בחירת הגופים המפוקחים נלקחו בחשבון היקפי המידע, כמות הלקוחות (נושאי המידע), ורגישות המידע במסגרת השירותים הניתנים ללקוחות. שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: (1) בקרה ארגונית (2) ניהול מאגרי מידע (3) אבטחת מידע (4) שימוש בשירותי מיקור חוץ. הציונים ניתנו לגופים בהתאם למענה שסופק לשאלונים, ולמסמכים שסופקו על ידם המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים, כאשר 30 גופים מתוך כלל הגופים נדרשו לבצע השלמת ידיעות ומסמכים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, תבדוק הרשות באמצעות ביקורת חוזרת את השלמת התיקונים, בהתאם לשיקול דעתה.

2.3. ליקויים, מסקנות והמלצות עיקריות

במגזר חברות הסיעוד נמצאה רמת עמידה בינונית במרבית הקריטריונים, ובשקלול הציונים של המפוקחים שניתנו לגבי מידת היענות שלהם לסעיפי החוק והתקנות, נמצא כי 52% מהמפוקחים הציגו רמה גבוהה של עמידה בהוראות החוק, 18% הציגו רמת עמידה בינונית ו- 30% מהמפוקחים הציגו רמה עמידה נמוכה של היענות לחוק. באופן פרטני, נמצא כי בכל הקשור לקריטריון הבקרה הארגונית הבוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום, רק 43% מכלל הגופים נמצאו ברמת עמידה גבוהה, בקריטריון ניהול מאגרי המידע הבוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר, ואיסוף של מידע ביומטרי, נמצאה רמת עמידה גבוהה של 64% מהגופים, כאשר ב-10% נמצאה רמת עמידה בינונית וב-26% נמצאה רמת עמידה נמוכה. בקריטריון אבטחת המידע הבוחן את עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם, רק כמחצית (54%) מהגופים עמדו בהוראות החוק והתקנות ברמת גבוהה, 17% מהגופים עמדו ברמה בינונית וכשליש (29%) מהגופים הציגו רמת עמידה נמוכה בקריטריון זה. רמת עמידה נמוכה במיוחד נמצאה בבדיקת קריטריון עיבוד מידע אישי במיקור חוץ, הבוחן בין היתר את אופן ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, ואת



האופן בו הם מבטיחים הגנה על המידע, בו 65% מהחברות שדיווחו כי משתמשות במיקור חוץ עבור עיבוד מידע, לא עמדו כלל בהוראות התקנות בכל הקשור לעיבוד מידע אישי במיקור חוץ ו-13% נמצאו ברמת עמידה חלקית.

נכח הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 39 מתוך 40, הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם, תוך הנחייה לתעדף את תיקון הליקויים, הן מבחינת בניית התכנית לתיקונם, והן מבחינת הטיפול בפועל, על בסיס גישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בקריטריונים של עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, ובקרה ארגונית.



ממצאי הליך פיקוח רוחב בקרב מגזר סיעוד

אתגרים ומאפיינים ייחודיים של מגזר סיעוד



פערי כוחות משמעותיים בן מבקשי המידע לבין המטופלים



מתקבל מידע בריאותי וסיעודי ממספר גורמים מדווחים (המטופלים, בני משפחתם, הביטוח הלאומי)



ניהול ואחזקת מאגרי מידע בהיקפים עצומים

התהליך שבוצע במספרים



39

הנחיות לתיקון ליקויים



30

דרישות להשלמת מידע חסר בכתב



6

גופים שבוצעה בהם ביקורת מעקב



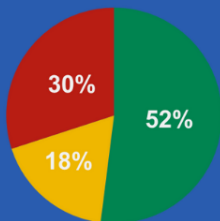
40

שאלונים שהופצו

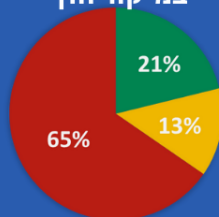
ממצאים - ליקויים מרכזיים

רמת עמידות גבוהה
רמת עמידות בינונית
רמת עמידות נמוכה

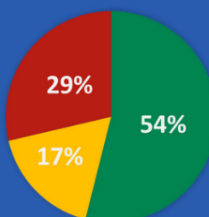
עמידה משוקלת



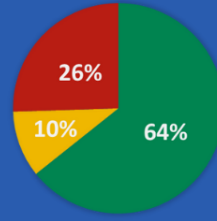
עיבוד מידע אישי במיקור חוץ



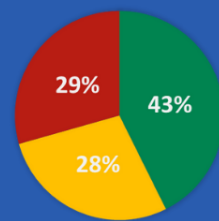
אבטחת מידע



ניהול מאגרי המידע



בקרה ארגונית



הליקויים המרכזיים שנמצאו, מדגישים את הצורך במינוי מנהל מאגר מידע לכל מאגר מידע הקיים בארגון, לרבות הוצאת כתב מינוי רשמי למנהל המאגר במקרים בהם נדרש מינוי כאמור, ובהתאם לסעיף 9 להוראות החוק.

על ארגונים להקפיד על עיגון נהלי אבטחת מידע, הכוללים את מלוא הנושאים המפורטים בתקנה 4 לתקנות אבטחת מידע.

נמצאו גופים אשר אין להם תיעוד מסודר לתכנית עבודה שנתיית לבקרה שוטפת על העמידה בדרישות התקנות ו/או שתוכנית העבודה אינה מכסה את הדרישות בתקנות.

נמצאו ליקויים בנושא ביצוע בדיקת התאמה לעובדים חדשים בעלי גישה למאגר אשר נועדה לוודא שאין חשש כי בעל הרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר.

על ארגונים לוודא כי קיים נוהל עבודה המסדיר את הליך הטיפול באירועי אבטחת מידע. נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח המיידי לרשות, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע. במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.

על הגורמים הרלוונטיים בארגונים לקיים דיון אודות הצורך בחיבור אמצעים נתיקים למערכות הארגון. ככל שיוחלט כי לא קיים צורך ממשי או קיים צורך מינימאלי, עליהם להגביל את השימוש באופן שיטאים לרמת האבטחה החלה על הארגון ורגישות המידע המנוהל. במקרים בהם יוגדר כי אכן קיים צורך בשימוש באמצעים נתיקים, יש להצפין נתונים באמצעות שיטות הצפנה מקובלות.

במאגרים שחלה עליהם רמת אבטחת בינונית ומעלה, אופן הזיהוי בכניסה למאגר מידע ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. למשל תעודה המכילה חתימה אלקטרונית מאובטחת, TOKEN וכו'.

במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לקבוע בנהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה.

לא מתבצע הליך של ביטול הרשאות במערכות המידע לעובדים אשר עזיבתם את מקום העבודה מיד עם עזיבתם כנדרש בתקנה 9(ג).

במרבית הארגונים לא בוצעו פעולות מספקות בהערכות להתקשרות עם גוף צד ג' למתן שירותי עיבוד מידע אישי במיקור חוץ כנדרש בתקנה 15 ובהנחיות רשם מאגרי המידע מס' 2/2011.

בחלק מארגוני הסיעוד לא קיימים או קיימים הסכמים חלקיים עם גוף צד ג', לגבי אופן עיבוד המידע האישי במיקור חוץ

נדרש כי ארגונים יגדירו מנגנוני בקרה ופיקוח במטרה לוודא כי צד ג' ממלא חובותיו בהתאם למוגדר בהסכם ההתקשרות, ביחס לדרישות הגנת הפרטיות



בעת פניה לקבלת מידע אודותיו לצורך שמירתם במאגר, יש להקפיד על מתן הודעה לנושא המידע בעת איסוף המידע, נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.



3. מגזר חברות הסיעוד - תמונת מצב

3.1. כללי

הדו"ח מתייחס לפיקוחי הרחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למאי 2020 במגזר חברות הסיעוד.

3.2. רקע על המגזר

במסגרת סקר רחבי במגזרי המשק שערכה הרשות להגנת הפרטיות, אשר בחן את סיכוני הפרטיות במגזרים השונים, מגזר חברות הסיעוד אותר כאחד מיעדי פיקוח הרחב המשמעותיים. מאגרי המידע של חברות הסיעוד כוללים מידע רפואי-סיעודי רגיש על מאות אלפי מטופלים, ובנוסף, ברשותם מאגרי מידע הכוללים אלפי רשומות המכילות נתונים אישיים אודות מטפלים המועסקים דרך אותן חברות הסיעוד.

מגזר חברות הסיעוד הינו בעל מאפיינים ייחודיים בהיבטי פרטיות, הבאים לידי ביטוי בין ביות, בהיבטים שלהלן:

- ניהול והחזקת מידע רגיש על מצבם הבריאותי של לקוחות חברות הסיעוד;
- ריכוז מידע בריאותי וסיעודי ממספר גורמים מדווחים (מטופלים, בני משפחתם, המוסד לביטוח לאומי וכד');;
- חברות סיעוד אשר חלק ניכר מהן בעלות מספר סניפים ברחבי הארץ ואשר משרתות אלפי לקוחות מחזיקות במאגרי מידע בהיקפים עצומים;
- פערי כוחות משמעותיים בין בעלי המאגרים לבין המטופלים, הנובעים מהעובדה שחלק מנושאי המידע בעלי תפקוד פיזי או קוגניטיבי נמוך, העלולים להתאפיין במודעות נמוכה לפרטיות, לסיכונים הנובעים משימוש במידע עליהם, או לזכויות המוקנות להם.

מבחינת סוגי הגופים הפועלים במגזר זה, זיהתה הרשות חלוקה של ארבעה סוגים של ארגונים:

- **חברות כוח אדם גדולות** - בהן חברות כוח אדם מובילות בשוק הישראלי, אשר מפעילות חברות-בת העוסקות בתחום הסיעוד. חלק מחברות אלו פועלות כחברות ציבוריות, בעלות עשרות סניפים ברחבי הארץ (בין 30-40 סניפים), מעסיקות בין 300 ל-700 עובדי מטה, ועשרות אלפי מטפלים המטפלים בעשרות אלפי לקוחות.
- **חברות סיעוד גדולות** - חברות העוסקות בתחום הסיעוד באופן בלעדי. מחזיקות בין 10 ל-25 סניפים בכל רחבי הארץ, מעסיקות בין 70 ל-250 עובדי מטה ובין 5,000 ל-10,000 מטפלים, עם אלפי עד עשרות אלפי לקוחות.

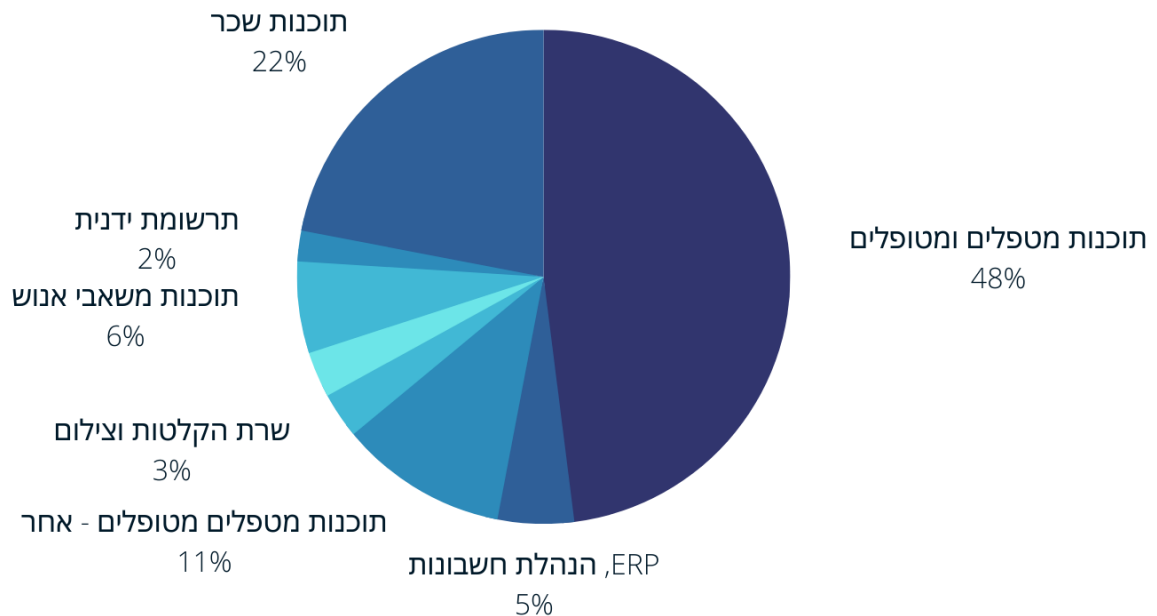




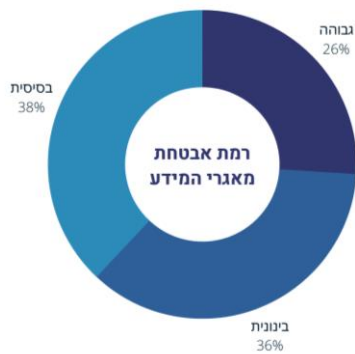
- **חברות סיעוד בינוניות** – חברות העוסקות בסיעוד או בסיעוד ודיר מוגן גם יחד. לרוב אינן בעלות פריסה ארצית אך מחזיקות בין 5 – 10 סניפים שונים. מעסיקות בין 10 ל-50 עובדי מטה, ובין מאות לאלפי מטפלים המעניקים שירותי סיעוד לאלפי מטופלים.
- **ארגוני סיעוד קטנים**-חברות משפחתיות או עמותות, אשר מחזיקות בין סניף ראשי בודד ועד ל-5 סניפים לכל היותר. מעסיקות פחות מ-10 עובדי מטה קבועים ומאות בודדות של מטפלים, המעניקים שירותי סיעוד למאות מטופלים.

ממצאי פיקוח הרחב מעלים כי חברות הסיעוד מנהלות ומחזיקות מגוון רחב של סוגי מידע שלמעלה ממחציתו הוא, כאמור, מידע על מטופלים. 77% מכלל חברות הסיעוד שנבדקו, עושות שימוש באחת משתי מערכות מידע עיקריות הייעודיות למגזר הסיעודי, לצורך ניהול מאגרי מידע של המטופלים והמטפלים¹. שימוש במערכות אלו עשוי לתרום לריכוז מידע אישי רגיש באופן בלתי מבוזר, ומכאן גם מחייב עמידה יתרה של הגופים בהוראות החוק והתקנות, בדגש על חובות הנובעות מעיבוד מידע אישי במיקור חוץ. בנוסף, גם החברות המעניקות את השירותים ותוכנות המדף מחויבות לעמוד בכל החובות הקבועות בחוק ובתקנות מעצם היותן מחזיקות במידע אישי רגיש, וביתר שאת, בהיותן מחזיקות בלמעלה מחמישה מאגרים.

מעבר למידע אודות המטופלים והמטפלים, החברות הפועלות במגזר זה מנהלות בין היתר גם מידע אודות עובדים שאינם מטפלים, נתוני שכר, מערכות לתכנון משאבי ארגוני (ERP) ובינה עסקית (BI) ואף מידע הכולל הקלטות אודיו ווידאו.



¹ תוכנת "תלם" המופצת ע"י משרד הרווחה, ותוכנת "אדם" המופצת ע"י חברת "מידע מחשבים פתרונות תוכנה בע"מ".



בהתאם לסיווג רמת אבטחת המידע כמפורט בתוספת לתקנות, נמצא כי מרבית הגופים שנבדקו במגזר זה מנהלים מאגרי מידע ברמת סיווג אבטחת מידע בינונית או גבוהה (72%) כאשר יתר הגופים מנהלים מאגרים ברמת סיווג (28%) בסיסית (38%). רמת אבטחת המידע הנדרשת למאגרים מתפלגת באופן דומה בין הרמות השונות של סוגי הגופים הפועלים במגזר זה, כאשר רמות העמידה הגבוהות

באבטחת המידע נמצאו בגופים להם מאות משתמשים בעלי גישה למאגרים, ורמות העמידה הבינוניות והנמוכות לגופים הבינוניים והקטנים להם מספר קטן יותר של מורשי גישה ונושאי מידע.

בין יעדי הפיקוח שנבדקו, נמצא כי צורת ההתאגדות השכיחה הינה חברה בע"מ (87% מהגופים שנבדקו), בעוד ששאר גופי הסיעוד שנבדקו (13%) מאוגדים כעמותות.

מאפיינים אלו, בצירוף פערי הכוחות בין הצדדים דורשים הקפדה מיוחדת מכלל חברות הסיעוד לעמידה בדרישות החוק, בדגש על הזכויות והדרישות הנובעות ממנו, וכן הקפדה יתרה על תקנות אבטחת המידע, לרבות קיום רמת אבטחת מידע גבוהה, הדרכות שוטפות ובקרה שוטפת אחר המידע הרגיש במאגרים.

3.3. תהליך העבודה

במטרה לפעול באופן המיטבי ביותר למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, נוקטת הרשות להגנת הפרטיות בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרחבת שיש לפעולותיה על המשק, על מנת לעמוד במכלול האתגרים העומדים לפתחה. הרשות פועלת על-פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכונים פרטיות ממקד את תחומי הפעילות של הרשות ומאפשר לה לעסוק, בין היתר, בתחומים בהם ישנה השפעה רחבת על מגזרים שונים, הכוללים מספר רב של משתמשים ומידע רגיש.

תוצרי הערכת המצב כוללים תופעות ומגזרים המתאפיינים בסיכונים מיוחדים לפרטיות, הממקדים את מוקדי העיסוק העתידיים של הרשות ואת תשתית תכנית העבודה שלה. כאמור, מגזר חברות הסיעוד מתאפיין בכמה סיכונים, לרבות ניהול והחזקת מידע רגיש על מצבם הבריאותי של לקוחות חברות הסיעוד; ריכוז מידע בריאותי וסיעודי ממספר גורמים מדווחים; פריסה ארצית וניהול מידע בהיקפים עצומים; פערי כוחות משמעותיים בין בעלי המאגרים לבין המטופלים. נוכח האמור, הוגדר מגזר חברות הסיעוד כאחד מיעדי פיקוח הרחב של הרשות.



בהליך הפיקוח פנתה הרשות בדרישה למילוי שאלון ביקורת ל- 40 גופים המנהלים חברות סיעוד. במסגרת בחירת הגופים נלקחו בחשבון היקפי המידע וכמות הלקוחות, וכן רגישות המידע במסגרת השירותים הניתנים ללקוחות. שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: **בקרה ארגונית, ניהול מאגרי מידע, אבטחת מידע, ושימוש בשירותי מיקור חוץ**. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, ומעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים, כאשר 30 גופים מתוך כלל הגופים נדרשו לבצע השלמת ידיעות ומסמכים.

בסיום הליך פיקוח הרחב ובהתאם לממצאים, נמצאו ליקויים הדורשים תיקון אצל 39 גופים מתוך 40 הגופים המפוקחים. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, ולהגיש לה מסמך המפרט את הליקויים אשר תוקנו, והתחייבות חתומה בידי נושא משרה בכיר בארגון לתיקון יתר הליקויים על פי תכנית עבודה מסודרת של הארגון ולוחות זמנים לביצוע. הגופים נתבקשו לתעדף את תיקון הליקויים, הן מבחינת התכנית, והן מבחינת הטיפול בפועל, על בסיס גישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בקריטריונים של עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, ובקרה ארגונית.

ככל שנה, מבצעת הרשות ביקורות מעקב אחר המגזרים שנבחנו במסגרת פיקוחי הרחב. במהלך שנת 2020 הפיצה הרשות ל-6 חברות סיעוד, המהוות 15% מסך הגופים שנבדקו, דרישת דיווח אודות יישום תכנית העבודה ותיקון הליקויים, ובחינת העמידה בלוחות הזמנים שהוקצו לכך, בהתייחס לכל אחד מהליקויים שנמצאו בהליך הפיקוח בארגון. החברות שנבדקו במסגרת פיקוח המעקב נבחרו על פי כמות הליקויים שאותרו בפיקוח הרחב ואופיים. נכון למועד פיקוח המעקב, 41% מהגופים שנבדקו בפיקוח המעקב דיווחו על תיקון מלא של הליקויים. 45% מהגופים שנבדקו בפיקוח המעקב מסרו לרשות מידע ונתונים לעניין הליקויים שנקבעו - מידע שלא נמסר בהליך הפיקוח הראשוני - לרבות ידיעות ומסמכים נוספים המניחים את הדעת ביחס לאופן העמידה של הגוף בהוראות החוק והתקנות. ב-14% מהגופים לא נמסר דיווח על תיקון הליקוי או שניתן הסבר חלופי או הסתייגות של הגופים בנוגע לעצם קביעת הליקוי הדורש בדיקת המשך. לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע להליכי אכיפה משלימים לרבות בכל הנוגע למסירת תכניות העבודה וליישומן.

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

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

- **בקרה ארגונית** - קריטריון זה בוחן את קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;





- **ניהול מאגרי מידע** - קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר, ואיסוף של מידע ביומטרי;
 - **עיבוד מידע אישי במיקור חוץ** - לרבות בחינת ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע;
 - **אבטחת מידע** - בחינת עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם;
- רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו חברות הסיעוד, וזאת בהתבסס על בחינת הרשות את תשובותיהן לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:
- עמידה של בין 80% - 100% בקריטריונים, מוגדרת כרמת עמידה גבוהה.
 - עמידה של בין 50% - 80% מוגדרת כרמת עמידה בינונית/חלקית.
 - עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

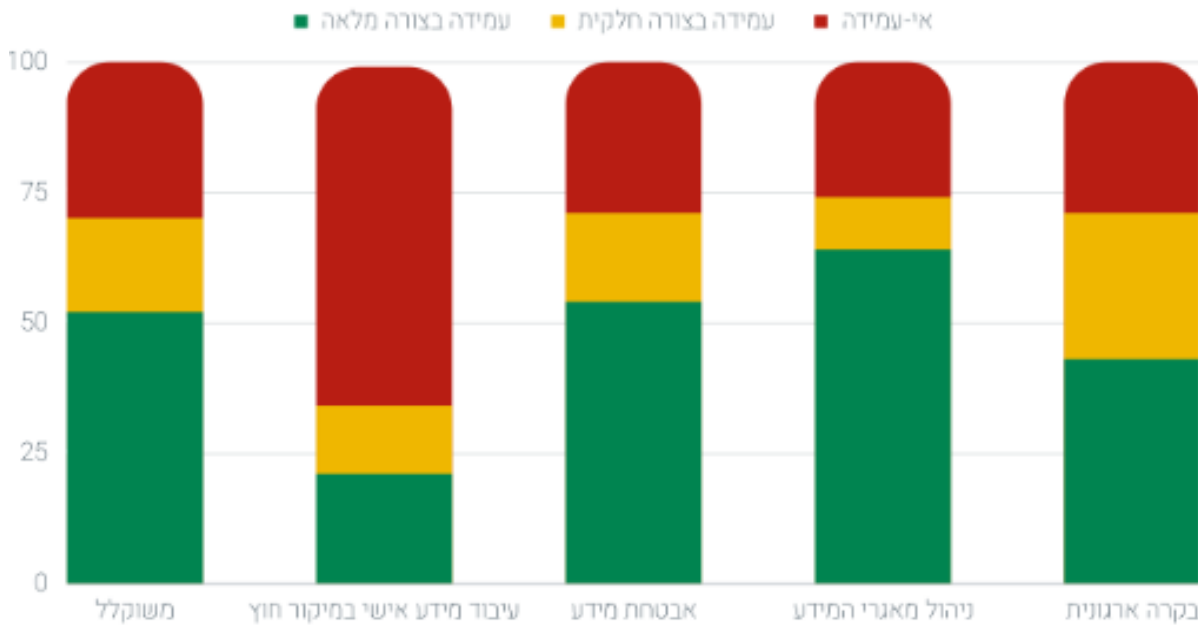
4. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי

ממצאי פיקוח הרחב העלו הבדלים משמעותיים באופי הפעילות בין הגופים השונים הפעילים בשוק, אשר, מכך משליך במישרין גם על רמת עמידתם בהוראות הדין. גיסא, המגזר כולל חברות קונצרניות המפעילות מערך מחשוב ומטה גדול ומשמעותי, בעלות פריסה ארצית רחבה ומעסיקות עד אלפי עובדים. ומאידך גיסא, ישנן חברות בינוניות וקטנות, המעסיקות מספר קטן יחסית של עובדי מטה, ובעלות יכולת ניהול מצומצמות של מערך המחשוב.

בחישוב מצרפי של כלל הגופים נמצא כי אצל מרבית חברות הסיעוד קיימת רמה בינונית עד גבוהה של עמידה בדרישות חוק הגנת הפרטיות ותקנותיו. עם זאת, נמצא כי אצל פחות ממצחית (48%) מהמפוקחים קיימת עמידה מלאה בדרישות החוק והתקנות. רמת עמידה נמוכה במיוחד זוהתה בטיפול במיקור חוץ של מאגרי מידע על ידי גורם חיצוני. בעניין זה רק 21% מהמפוקחים עמדו בצורה מלאה בדרישות החוק בנושא עיבוד מידע אישי במיקור חוץ. בנוסף, רמת עמידה נמוכה נמצאה גם בבחינת תחום הבקרה הארגונית, בו 57% מהמפוקחים עמדו בדרישות החוק בצורה חלקית או שלא עמדו כלל. בתחום אבטחת המידע נמצא כי רק 54% מהחברות עמדו בדרישות החוק בצורה מלאה.



ריכוז הממצאים ברמת יעד פיקוח הרחב, ולפי התחומים שנבדקו:



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

4.1. בקרה ארגונית



- במסגרת בחינת קריטריון זה, נמצא כי רק 43% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לבקרה ארגונית, בעוד ש-57% נמצאו כבעלי רמת עמידה בינונית ונמוכה בהוראות החוק כאמור.
- ב-92% מהגופים לא מונה מנהל מאגר או שחסרים כתבי מינוי פורמאליים כנדרש, או שכלל לא התקבל מידע בנושא.
- ב-64% מארגוני הסיעוד שנבדקו, אין כלל נוהל אבטחת מידע או שהנהלים שהתקבלו אינם מקיפים את כלל הדרישות בהוראות התקנות.
- בלמעלה ממחצית מהגופים שנבדקו (51%), לא נמצאה תכנית עבודה שנתית לבקרה שוטפת על העמידה בדרישות התקנות, או שתוכנית העבודה שנמצאה אינה מכסה את הדרישות בתקנות.

4.2. ניהול מאגרי מידע



- במסגרת בחינת קריטריון זה, נמצא כי 64% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לניהול מאגרי מידע, בעוד ש-36% נמצאו כבעלי רמת עמידה בינונית ונמוכה בהוראות החוק בנושא זה.

- מן הממצאים עלה כי ב-18 גופים נמצאו ליקויים בכל הקשור לחובת השקיפות בנוגע למקור הסמכות

לאיסוף המידע האישי, ואי עמידה בחובת יידוע נושאי המידע שעליהם מוחזק המידע, בדבר זכויותיהם בהתאם לסעיף 11 לחוק, בעת פניה לקבלת מידע.

- בחלק מהגופים לא ניתנה לנושא המידע האפשרות לעיין במידע אודותיו לפי בקשתו כנדרש בסעיף 13 לחוק, ואף לא ניתנה האפשרות לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק.

4.3. אבטחת מידע



- במסגרת בחינת קריטריון זה, נמצא כי כמחצית (54%) מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לאבטחת מידע, במחצית השנייה של הגופים (46%) נמצאה רמת עמידה בינונית ונמוכה בכל הנוגע ליישום הוראות החוק והתקנות בנושא (17% מהגופים נמצאו כבעלי רמת עמידה בינונית ו-29% מהגופים ברמת עמידה נמוכה).

- ב-51% מהגופים נמצאו ליקויים בנושא אבטחת אמצעים נתיקים, בין אם בהעדר הגבלות על שימוש באמצעים אלו, או בהעדר הצפנה נאותה.

- ב-14 גופים (כ-36%), ושחלה עליהם רמת אבטחה גבוהה, לא בוצעו כנדרש או שלא בוצעו כלל ביקורות אבטחת מידע או מבדקי חדירות אשר חלה חובה לבצעם.

- ב-41% מהגופים, לא נשמר תיעוד של אירועים המעלים חשש לאירוע אבטחה כנדרש בתקנה 11 לתקנות.

- ב-36% מהגופים שחלה עליהם רמת אבטחה בינונית או גבוהה לפי התקנות, אשר מאפשרים כניסה למאגר המידע באמצעות רשת האינטרנט, לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לדרישת תקנה 9(ב)(1).

- ב-82% מהגופים נמצא כי במרבית מערכות המאגר לא קיימת מדיניות סיסמאות חזקה, הכוללת סיסמאות מורכבות או החלפות תקופתיות של סיסמאות כנדרש בתקנות. בשיעור זה מהגופים לא מתבצע הליך של ביטול הרשאות במערכות המידע לעובדים אשר עוזבים את מקום העבודה.

4.4. עיבוד מידע אישי במיקור חוץ

- 
- במסגרת בחינת קריטריון זה, נמצא כי 21% בלבד מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לעיבוד מידע אישי במיקור חוץ, בעוד ש-79% נמצאו כבעלי רמת עמידה בינונית ונמוכה.
 - ב-11 ארגוני סיעוד (כ-28%), לא ננקטו צעדים מספקים מבעוד מועד על מנת להעריך את מידת הסיכון הנשקפת למידע, ולפגיעה אגב כך בזכותם לפרטיות של נושאי המידע, כפועל יוצא מהשירותים הניתנים על ידם במיקור חוץ.
 - מבין 11 הגופים הנ"ל, נמצא כי הגופים אינם מבצעים התקשרות עם ספקי מיקור חוץ בהתאם לדרישות הקבועות בתקנות, כלומר, לא בוחנים את איכות ניהול אבטחת המידע ואת אופן תפעול מאגרי המידע אצל ספקי המיקור החוץ ולא מבצעים פעולות פיקוח כנדרש בהתאם להוראות תקנה 15 לתקנות.

5. מסקנות/תמונת מצב והמלצות

ממצאי הליך פיקוח הרחב עולה כי הגם שמרבית הגופים במגזר הסייעוד בעלי היכרות עם דרישות החוק והתקנות, והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, **עדיין נמצאו ליקויים משמעותיים באופן יישום הוראות החוק והתקנות. הנחיית הרשות היא כי על הגופים המשתייכים למגזר זה ליישם את הנקודות הבאות:**

5.1 בקרה ארגונית

- נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים הפועלים במגזר זה, בין היתר, לוודא את רישום כלל מאגרי המידע שבעלותם, לרבות התאמה בין זהות מנהל המאגר על פי מסמכי הארגון, לבין הרישום אצל רשם מאגרי המידע.
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות עדכון פרטי מנהל המאגר בפנקס המאגרים ככל שמונה כזה, וכן מינוי ממונה אבטחת המידע. בנוסף, יש לוודא שכתב המינוי כולל את כל הפרטים הנדרשים בהתאם להוראת סעיף 7 לחוק ולתקנה 4 לתקנות.
- בהתאם להוראות התקנות, יש לבצע הדרכות לגורמים האמורים אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. תיעוד החומרים שהועברו וכן התיעוד לביצוע ההדרכות – יישמר.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון. על הנהלים לכלול התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכד'. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות (תקנה 4).
- כמו כן, יש לוודא קיומה של תכנית עבודה לנושא אבטחת מידע והגנת הפרטיות, לרבות התייחסות לנושא גורם אחראי ולוחות זמנים לביצוע, שתעמוד בדרישות התקנות (תקנה 3(3)). ככל שמדובר בגוף שחלה עליו רמת האבטחה הגבוהה וככזה הוא חייב במבדקי חדירות, עליו לוודא כי הללו אכן בוצעו וכי הם עומדים בדרישות התקנות (תקנה 16).
- בנוסף, בהתאם לנדרש בתקנות (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים, או כל גורם אחר שמקבל גישה למאגר או למערכת הכוללת מספר מאגרים.

5.2 ניהול מאגרי מידע

- יש ליידע את בעל המידע בדבר המקור החוקי לאיסוף המידע על אודותיו, ובכל מקום שאין סמכות חוקית כזו, לקבל את הסכמתו עבור שמירת פרטיו במאגרים. זאת, תוך מתן הודעה בעת איסוף המידע לפי סעיף 11 לחוק, הכוללת התייחסות לשאלה האם חלה עליו חובה חוקית למסור את



המידע כאמור, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.²

- על הגופים להקפיד לאפשר לנושאי המידע לעיין במידע על אודותיהם המוחזק במאגר מידע, בהתאם לסעיף 13 לחוק. לעניין זה, יודגש כי זכות העיון חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות, תכתובות צ'ט, שיחות המצלמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי. כמו כן, יש להקפיד לאפשר לנושאי המידע לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע, בהתאם לסעיף 14 לחוק.

5.3. אבטחת מידע

- על הגופים לוודא קיומם של נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, וכן לוודא כי הנהלים נבחנים מחדש מעת לעת כנדרש בתקנות
- על הגופים לבחון את הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – מוצע להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד למערכת, ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.
- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות אבטחת מידע. עוד יש לוודא כי פרק הזמן לשמירת תיעוד שמאפשר ביקורת על הגישה למערכות המאגר הינו לפחות 24 חודשים, כנדרש בתקנה 10 לתקנות

5.4. עיבוד מידע אישי במיקור חוץ

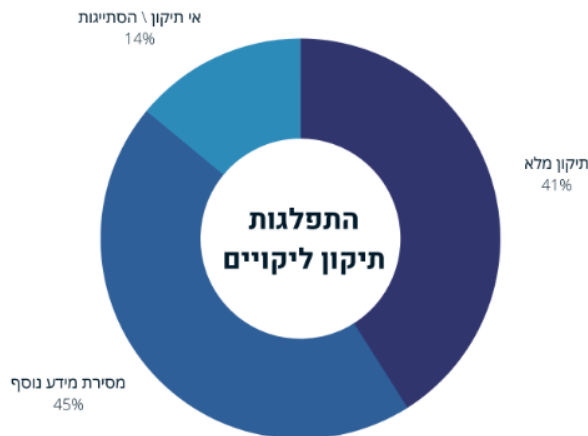
- בהתאם לתקנה 15 לתקנות על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות. בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל ההוראות המתחייבות על פי תקנה 15(א)(2) לתקנות, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- בעניין זה יש לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2/2011.³

² להרחבה בנוגע לחובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות, ראו מסמך בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" שפרסמה הרשות להגנת הפרטיות במאי 2022 להערות הציבור. המסמך זמין כאן.

³ הוראות דומות לעניין החובות המוטלות על בעל מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי". ההנחיה זמינה כאן.

6. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

בסיום הליך פיקוח הרחב כאמור, הגופים שבהתנהלותם נתגלו ליקויים הונחו להגיש לרשות בתוך זמן קצוב מסמך המפרט את הליקויים אשר תוקנו, והתחייבות חתומה בידי נושא משרה בכיר בארגון לתיקון יתר הליקויים, על פי תכנית עבודה מסודרת של הארגון הכוללת לוחות זמנים לביצוע.



במסגרת פיקוח הרחב במגזר זה נמצאו סה"כ 364 ליקויים ב-39 הגופים, שתיקונם נדרש על ידי הרשות. חלק מהליקויים דורשים תכנון רב שנתי או היערכות ארוכה להטמעתם בכלל מאגרי הגופים, בהתאם לסדרי העדיפויות שקבעה הרשות. משכך, בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים ואת העמידה בלוחות הזמנים שהגדירו ליישום התכנית ותיקון יתרת הליקויים שטרם תוקנו.

בטיפול בתיקון הליקויים נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בקריטריונים של עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, בקרה ארגונית וממשל תאגידי והעברת מידע בין גופים ציבוריים.

מדי שנה, מבצעת הרשות ביקורות מעקב אחר המגזרים שנבחנו במסגרת פיקוחי הרחב. במהלך שנת 2020 הפיצה הרשות ל-6 חברות סיעוד, המהוות 15% מסך הגופים שנבדקו, דרישת דיווח אודות יישום תכנית העבודה ותיקון הליקויים, ובחינת העמידה בלוחות הזמנים שהוקצו לכך, בהתייחס לכל אחד מהליקויים שנמצאו בהליך הפיקוח בארגון. החברות שנבדקו במסגרת פיקוח המעקב נבחרו על פי כמות הליקויים שאותרו בפיקוח הרחב ואופיים. נכון למועד פיקוח המעקב, 41% מהגופים שנבדקו בפיקוח המעקב דיווחו על תיקון מלא של הליקויים. 45% מהגופים שנבדקו בפיקוח המעקב מסרו לרשות מידע ונתונים לעניין הליקויים שנקבעו - מידע שלא נמסר בהליך הפיקוח הראשוני - לרבות ידיעות ומסמכים נוספים המניחים את הדעת ביחס לאופן העמידה של הגוף בהוראות החוק והתקנות. ב-14% מהגופים לא נמסר דיווח על תיקון הליקוי או שניתן הסבר חלופי או הסתייגות של הגופים בנוגע לעצם קביעת הליקוי הדורש בדיקת המשך. לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע להליכי אכיפה משלימים לרבות בכל הנוגע למסירת תכניות העבודה וליישומן.



ביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, רשאית הרשות להטיל סנקציות נוספות העומדות לרשותה מכוח החוק.

מממצאי פיקוח המעקב עלה כי מרבית הגופים תיקנו מספר ליקויים משמעותי מתוך כלל הליקויים שנמצאו בפיקוח הרחב הראשוני.

פיקוחי המעקב שבוצעו במגזר חברות הסיעוד מעידים באופן חד משמעי על כך כי עצם קיום הליכי פיקוח הרחב מהווה תמריץ לגופים השונים לבצע הליך בחינה עצמית באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרחב.

7. סיכום

מגזר חברות הסיעוד הינו בעל מאפיינים ייחודיים בהיבטי פרטיות, הבאים לידי ביטוי בין היתר בהחזקת וניהול מידע רגיש על מצבם הבריאותי של לקוחות חברות הסיעוד, ריכוז מידע בריאותי וסיעודי ממספר גורמים מדווחים, פריסה ארצית ושירות אלפי לקוחות, החזקת מאגרי מידע בהיקפים עצומים ופערי כוחות משמעותיים בין בעלי המאגרים לבין המטופלים.

ממצאי הליך פיקוח הרחב במגזר חברות הסיעוד העלה ממצאים מדאיגים המצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ, ועמידה חלקית בהוראות החוק בכל הנוגע לתקנות אבטחת מידע. בנוסף, נמצא כי חלק מהגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את ציבור המטופלים בדבר זכויותיהם על פי חוק הגנת הפרטיות ונוכח פערי הכוחות במגזר זה, עליהם להקפיד ביתר שאת בכל הנוגע לאופן קבלת ההסכמה בעת איסוף המידע, בהתאם לקבוע בסעיף 11 לחוק.

ניכר, כי עצם קיום הליך פיקוח הרחב עורר אצל הגופים שנבדקו תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחיבות נושא משרה ותכנית מסודרת לתיקון הליקויים.

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

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר הסיעוד, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.





8. נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית			
לא בוצע סקר סיכונים או ביקורות בנושא אבטחת מידע והגנת הפרטיות בשלוש השנים האחרונות	השלמת התהליך בהקדם וביצוע ביקורת בנושא אבטחת מידע וכן סקר סיכונים. עריכת ביקורות בנושא אבטחת מידע והגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה. לחלופין במאגר ברמת אבטחה גבוהה - עריכת סקר סיכונים מידי 18 חודשים הכולל את דרישות הביקורת.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5, תקנה 16	סקר סיכונים/ביקורת אבטחת מידע
עובדים חדשים אינם עוברים בדיקת התאמה.	הטמעת תהליך מיון של עובדים חדשים שבוחן היבטים הרלבנטיים לפרטיות ולאבטחת מידע.	אבטחת מידע בניהול כוח אדם –קליטת עובדים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 7	מיון עובדים חדשים
ממונה אבטחת המידע ממלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים במילוי תפקידו	יש למנות כממונה אבטחת מידע אדם בעל הידע המתאים, שאינו ממלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים במילוי תפקידו.	פרטי הממונה על אבטחת המידע חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3.	מינוי ממונה אבטחת מידע
לא קיים נוהל אבטחת מידע או שהוא כולל פחות מ-50% מהסעיפים המופיעים בתקנות.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם לנוהל.	נוהל אבטחת מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4 (ה)	נהלי אבטחת מידע
לא קיימת תכנית עבודה שנתית	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות המפרטת את הגורם האחראי ואבני דרך ברורות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	תכנית עבודה שנתית
עובדים חדשים לא עוברים הדרכה או שתדירות ההדרכות היא פחות מפעם בשנתיים או שההדרכות אינן מכסות את נושא אבטחת מידע והגנת הפרטיות בצורה מספקת-	יש לקבוע הדרכות לפחות פעם בשנתיים במאגרים שחלה עליהם רמת האבטחה הבינונית או הגבוהה בנושא אבטחת מידע והגנת הפרטיות בצורה מספקת וניהול תיעוד ומעקב אחר הדרכות אלו.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(ג)	הדרכות לעובדים



נושא	הפניה לחוק/תקנה/הנחיה	פעילות מתקנת נדרשת	הליקוי/פער
תכנית עבודה שנתית	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות המפרטת את הגורם האחראי ואבני דרך ברורות.	לא קיימת תכנית עבודה שנתית
ניהול מאגרי מידע			
מתן הודעה לנושא המידע	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11	מתן הודעה לתושב בעת איסוף המידע. על נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.	לא ניתנת הודעה בהתאם לדרישות סעיף 11 לחוק.
עיון במידע	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13	יש לאפשר לנושא המידע לעיין במידע שעליו המוחזק במאגר המידע.	לא ניתן לנושא המידע לעיין במידע על אודותיו כנדרש בסעיף 13 לחוק, או שניתנת לו אפשרות לעיין באופן חלקי בלבד
שינוי/תיקון המידע	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 14	יש לאפשר לתושב לתקן את המידע המוחזק בעניינו ברשות, אם נמצא כי המידע אינו נכון, שלם, ברור או מעודכן.	לא מתאפשר לנושא המידע לבקש לשנות או לתקן המידע אודותיו לפי סעיף 14 לחוק בשיעור גבוה מהרשויות
רישום המאגר אצל רשם	חוק הגנת הפרטיות תשמ"א – 1981, סעיף 8	יש לפעול להסדרת רישום מאגרי המידע בהקדם.	לא קיים רישום מאגרים של מטופלים בפנקס מאגרי המידע.
אבטחת מידע			
אבטחה פיזית	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 6	יש להבטיח כי המערכות יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות ושל כל הכנסה והוצאה אל מערכות המאגר ומהן.	אין אמצעי אבטחה פיזיים למניעת גישה לשרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע.



נושא	הפניה לחוק/תקנה/הנחיה	פעילות מתקנת נדרשת	הליקוי/פער
הצפנת התקנים ניידים	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 12	הגבלת או מניעת אפשרות לחיבור התקנים ניידים, התרת שימוש בהתקנים ניידים תוך שימוש בשיטות הצפנה מקובלות כאמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.	קיימת אפשרות לחבר התקנים ניידים ואין הצפנה.
אבטחת תקשורת	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 14 (א)	התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב במאגר המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת בהתאם לדרישות התקנות.	אין אמצעי הגנה למאגרים המחוברים לאינטרנט.
הפרדת מאגרים עם מידע שונה	ניהול מאובטח ומעודכן של מערכות המאגר תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב)	יש לקיים הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	לא קיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי ליתר המאגרים
מנגנון הרשאות	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 8, תקנה 9	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	לא קיים מנגנון הרשאות או שמנגנון ההרשאות מאפשר לבעלי תפקידים לגשת לנתונים במאגר למרות שאין בכך צורך
מנגנון הרשאות	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 8, תקנה 9 (א)	יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת (בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות) ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	לא ננקטים אמצעים סבירים לצורך ווידוא כי הגישה למאגרים נעשית בידי בעלי ההרשאה בלבד למאגר המידע/מערכת מידע.
שימוש באמצעי פיזי מרחוק	אבטחת תקשורת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 14 (ג). תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 9 (ב)(1).	במאגרים שחלה עליהם רמת אבטחתה בינונית ומעלה, אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. כגון תעודה המכילה חתימה אלקטרונית מאובטחת, TOKEN וכדומה.	בכניסה למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.
מבדקי חדירה	מבדקי חדירות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ד)	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה אחת לשנה וחצי, בחינת הצורך בעדכון נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.	לא נערכו מבדקי חדירה בשלוש השנים האחרונות על ידי גורם מקצועי.



הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא קיימת מדיניות סיסמאות חזקה.	במאגרים בעלי רמת אבטחה בינונית ומעלה, קביעה בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה, הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכדומה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב)	מדיניות סיסמאות
העברת מידע ממאגרי המידע ברשת ציבורית או ברשת האינטרנט לא נעשית באמצעות שימוש בשיטות הצפנה מקובלות.	העברת מידע ממאגרי המידע ברשת ציבורית או ברשת האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 14 (ב)	הצפנה
חלק מהמערכות לא נתמכות על ידי השרתים ומערכות ההפעלה	יש להחליף את התוכנות שאינן נתמכות בגרסאות עדכניות.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 13 (ג)	עדכון מערכות המאגר
קיימים מאגרים בהם לא קיים מנגנון ניתוק כאשר אין פעילות.	ברמת אבטחה בינונית ומעלה, נדרשת הגדרת ניתוק אוטומטי במערכות מאגרי המידע לאחר פרק זמן סביר של אי פעילות במערכת	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 9 (ב)2	ניתוק אוטומטי
לא מנוהל מנגנון תיעוד אוטומטי המאפשר ביקורת על הגישה למאגרים.	יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע, אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, תקנה 10	תיעוד גישה
לא נערך סקר סיכונים בשנה וחצי האחרונות	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים מדי שנה וחצי, ותיקון הליקויים שהתגלו במסגרת הסקר.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ג)	סקר סיכונים
לא קיים תיעוד של אירועי אבטחה.	יש לתעד כל אירוע המעלה חשש לאירוע אבטחה. בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחה מידע. במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.	תיעוד של אירועי אבטחה תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 11	תיעוד אירועי אבטחה



הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא קיים תהליך שמירה או גיבוי ללוג אבטחת המידע, או שמשך שמירת הגיבוי לא תואם לתקנה.	במאגרים בעלי רמת אבטחה בינונית או גבוהה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, וקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר באופן שיבטיח שניתן יהיה, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי בהתאם לתקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 17 (ב) ותקנה 18	גיבוי נתוני אבטחה
מיקור חוץ			
לא עוגנו הסכמי התקשרות עם ספקי מיקור חוץ המכילים את מלוא הפרטים הנדרשים בהתאם לתקנות.	יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות: 1. דיווח אודות אירועי אבטחת מידע. 2. מנגנוני אבטחת המידע הנדרשים. 3. שמירת המידע לאחר סיום תקופת ההתקשרות. 4. חובות גורם חיצוני בהעברת מידע לאחר.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	מיקור חוץ
לא קיים הסכם מול ספק מיקור החוץ.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 והנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי בחברה, לרבות נקיטת אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	מיקור חוץ
לא ננקטות פעולות לוודא כי גורם חיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש.	ווידוא כי כל גורם חיצוני אשר נותן שירותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15	מיקור חוץ