הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר בתי אבות והוסטלים

טבת תשפ"ג

ינואר 2023

תוכן

תקציר מנהלים

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

1.1. מגזר בתי אבות והוסטלים

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות אשר בוחן את סיכוני הפרטיות במשק, מגזר בתי האבות וההוסטלים אותר כאחד מיעדי פיקוח הרוחב המשמעותיים, ומתאפיין בעיקר בשלושה סוגי פעילות: 1. רשתות בעלות סניפים הפרוסים ברחבי הארץ. 2. מרכזים בעלי סניף אחד בלבד והיקף פעילות של בתי אבות והוסטלים שאינם פועלים במסגרת רשת ומעניקים טיפול לקבוצת אנשים מצומצמת. 3. חברות קשורות המעניקות שירותי בתי אבות והוסטלים לצד שירותים סיעודיים.

מגזר זה מעניק ללקוחותיו שירותי סיעוד וטיפול ובמסגרת זו, באופן טבעי, מקבל לידיו מידע רגיש על מצבם הרפואי, ועל כן הינו מגזר בעל מאפיינים ייחודיים בהיבטי פרטיות: : ריכוז מידע רפואי-סיעודי אודות דיירים נוכחים וקודמים ונתונים אודות דיירים שנפטרו. מאפיין נוסף הוא פערי כוחות משמעותיים בין בעלי המאגרים לבין הדיירים, 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.

1.2. תהליך העבודה

בהליך פיקוח הרוחב במגזר זה, פנתה הרשות לגופים המנהלים בתי אבות והוסטלים בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע, כמות הדיירים, ורגישות המידע הנאסף במסגרת השירותים הניתנים לדיירים. בסופו של יום, השיבו 31 גופים לשאלוני הפיקוח לאחר שהתברר כי חלק מהגופים סיימו פעילותם, שינו את תחום פעילותם, נמצאו ככאלו שאינם עובדים עם מערכות ממוחשבות, וחלקם השיבו מענה מאוחד בשל פעילות עסקית מאוחדת, ניהול מאגר משותף או תשתית טכנולוגית משותפת. 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.

לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר בתי אבות והוסטלים נמצאה רמת עמידה נמוכה במרבית הקריטריונים, בעיקר בתחומי שימוש בשירותי מיקור חוץ ובקרה ארגונית. בשקלול הציונים שניתנו לגבי מידת ההיענות להוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 67%.

ביתר פירוט, ממצאי הליך פיקוח הרוחב מלמדים על חוסר בקיאות מספקת בדרישות תקנות אבטחת מידע. יצוין, כי ממצאי פיקוח הרוחב העלו כי רמת העמידה בדרישות אבטחת המידע נמוכה באופן מובהק בקרב מוסדות בתי האבות וההוסטלים הפרטיים המטפלים בקבוצת מטופלים מצומצמת, זאת בהשוואה לרשתות הגדולות.

בהתייחס למידע האישי שבבעלות בתי האבות וההוסטלים ובהחזקתם, נמצא כי הגופים במגזר כלל אינם מודעים לחובות החלות עליהם כאשר הם מתקשרים עם צדדים שלישיים המחזיקים או מעבדים עבורם מידע אישי. כמו כן, בפיקוח הרוחב אותרו מקרים בהם גופים אשר ניהלו בתי אבות ניהלו גם גופים המשתייכים למגזר חברות הסיעוד (או להפך), דבר הדורש הקפדה יתירה על הפרדת המאגרים, השימושים ומורשי הגישה.

ממצאי פיקוח הרוחב העלו כי חלק מהגופים המפוקחים נוהגים לשמור מידע אודות דיירים שהלכו לעולמם או שעזבו, דבר העשוי ליצור סיכוני אבטחת מידע מיותרים והפרה של הוראות חוק הגנת הפרטיות. בהמשך הדו"ח יובאו המלצות הרשות בנושא.

במסגרת הבדיקה נמצא כי חלק מבתי האבות מסונפים ל-9 רשתות. ב-6 מהרשתות נמצא כי קיים ניהול מרכזי של מערכות המידע ועמו ניהול מרכזי של מאגרי המידע. ואילו ב-3 רשתות הנותרות, נמצא כי קיים ניהול מבוזר של מערך המחשוב, תוך פיצול של מאגרי המידע לרמת הסניף, שבו צומצמה כמות בעלי ההרשאות למאגר המקומי, ובהתאם ירדה לכאורה רמת סיווג אבטחת המידע של המאגר למרות שקיימת גישה כללית על ידי הסניף המרכזי. באופן זה, נוצר מצב שבו לכאורה, הארגון פטר את עצמו מהצורך בניהול מאגרים ברמת אבטחת מידע גבוהה.

בעניין זה עמדת הרשות היא כי רמת אבטחת המידע הנדרשת של מאגרי המידע לא משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר לפי התקנות הינו <u>סך כל בעלי ההרשאה</u> לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.

נוכח הממצאים שעלו מהליך פיקוח הרוחב, **כל הגופים שנבדקו (31 גופים), קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.**

ממצאי הליך פיקוח רוחב
בקרב מגזר בתי אבות והוסטלים

אתגרים ומאפיינים ייחודיים של מגזר בתי אבות והוסטלים

פערי כוחות בין נותן השירות ומוסר המידע

בתי אבות והוסטלים עשויים לאסוף מידע פרטי רב ורגיש אודות דיירים לרבות מידע רפואי, מידע על מצב כלכלי וכיוצ"ב אודות דיירים ונפטרים

הסתמכות רבה על שירותים חיצוניים, כגון חברות חיצוניות המעניקות שירותים עיבוד ואחסון מידע המחזיקות במאגרי הגופים

התהליך שבוצע במספרים

40
שאלונים שהופצו

9
גופים שהוסרו מהפיקוח

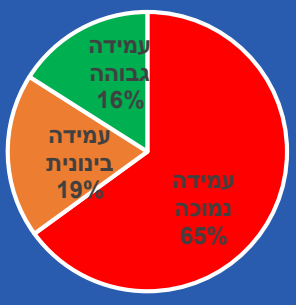
10
דרישות להשלמת מידע חסר בכתב

31
הנחיות לתיקון ליקויים

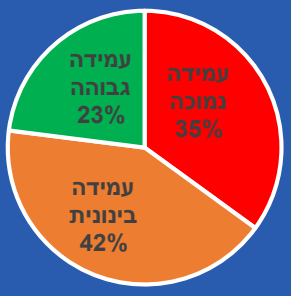
ממצאים – ליקוים מרכזיים

רמת עמידה גבוהה
רמת עמידה בינונית
רמת עמידה נמוכה

בקרה ארגונית



אבטחת מידע



- בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), יש לבצע בחינה של כלל הפעולות הנדרשות עבור כל גוף צד ג' אשר נותן שירותי עיבוד מידע אישי בחברה, ולהסדיר חובותיו של צד ג' בהיבט עמידה בתקנות במסגרת הסכם ההתקשרות. זאת ועוד, נדרש כי ארגונים יגדירו מנגנוני בקרה אקטיביים וזאת במטרה לוודא כי צד ג' ממלא חובותיו בהתאם למוגדר בהסכם ההתקשרות, ביחס לדרישות הגנת הפרטיות.

- יש למנות מנהל לכל מאגר מידע הקיים בארגון. לרבות הוצאת כתב מינוי רשמי למנהל המאגר במקרים בהם נדרש מינוי כאמור, ובהתאם לסעיף 9 להוראות החוק.
- על הארגונים להקפיד על עיגון נהלי אבטחת מידע, הכוללים את מלוא הנושאים המפורטים בסעיף 4 לתקנות. בנוגע לנוהל, יש להקפיד על כתיבת נוהל מלא הממצה בצורה מקיפה ומלאה את התקנה.
- לצורך עמידה בסעיף 7 לתקנות, על הארגונים לבצע הדרכות לעובדים בנושא הגנת הפרטיות ו/או אבטחת מידע בתדירות של אחת לשנתיים לכל הפחות, תוך שמירת תיעוד סדור לתוכן המועבר.

- יש להקפיד על מתן הודעה לנושא המיז
על נוסח ההודעה לכלול את כל המו
ובכלל זה התייחסות לשאלה האם חלו
חוקית למסור את המידע, או שמסירת
ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.

להקפיד לתעד כל אירוע המעלה חשש לאירוע
דא כי קיים נוהל עבודה המסדיר את הליך הטיפול
חת מידע. נוהל העבודה יכלול התייחסות לפעולות
ביצוע, 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.

- על הגורמים הרלוונטיים בארגונים לקיים דיון אודות הצורך בחיבור אמצעים נתיקים למערכות הארגון.
- במאגרים שחלה עליהם רמת אבטחה בינונית ומעלה, אופן הזיהוי בכניסה למאגר מידע ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לקבוע בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של הניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, וקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי בהתאם לסעיפים 18-17 לתקנות.

מגזר בתי אבות והוסטלים - תמונת מצב

כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למרץ 2020 במגזר בתי אבות והוסטלים, ולביקורות מעקב על פיקוחים אלו שבוצעו בתקופה שבין החודשים ינואר-מרץ 2021.

רקע על מגזר בתי אבות והוסטלים

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר בתי אבות והוסטלים כיעד פיקוח רוחב משמעותי, וזאת בשל מספר מאפיינים הייחודיים למגזר.

מגזר בתי האבות וההוסטלים מתאפיין בעיקר בשלושה סוגי פעילות: 1. רשתות בעלות סניפים הפרוסים ברחבי הארץ. 2. בתי אבות והוסטלים שאינם משויכים לרשת המעניקים טיפול לקבוצת אנשים מצומצמת. 3. חברות קשורות המעניקות שירותי בתי אבות והוסטלים לצד שירותי סיעוד.

מגזר זה מעניק ללקוחותיו שירותי סיעוד וטיפול ובמסגרת זו, באופן טבעי, מקבל לידיו מידע רגיש על מצבם הרפואי, ועל כן הינו מגזר בעל מאפיינים ייחודיים בהיבטי פרטיות: ריכוז מידע רפואי-סיעודי אודות דיירים נוכחים וקודמים ונתונים אודות דיירים שנפטרו. מאפיין נוסף הוא פערי כוחות משמעותיים בין בעלי המאגרים לבין הדיירים, הנובעים מהעובדה שלחלק מנושאי המידע תפקוד פיזי או קוגניטיבי נמוך, העלול להתאפיין גם במודעות נמוכה לזכויות המוקנות להם, ובתוך כך ולסיכונים המשמעותיים לפרטיותם הנובעים משימוש במידע עליהם.

תהליך העבודה

במטרה לפעול באופן המיטבי למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות נוקטת בגישה מבוססת סיכון, הבוחנת תדיר את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש לפעולותיה על המשק. הרשות פועלת על פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל המשק. על מנת לעמוד במכלול האתגרים העומדים לפתחה, פועלת הרשות על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, במגזרים שונים הכוללים מספר רב של נושאי מידע ומידע רגיש, וליישם את ממצאי הפעילות בצורה רוחבית.

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בבניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לתחומים שבסיכון מוגבר לפרטיות שזיהתה הרשות, ולמדיניות השנתית של הרשות. התוכנית נבנית בהתחשב בכמות והיקף המידע במגזר, רמת

רגישות המידע, מידע שהצטבר ברשות בנוגע לאותו מגזר או נושא, תלונות ספציפיות שהתקבלו ברשות, והצורך בבחינה מגזרית והבאת המגזר לרמת עמידה נאותה.

הליך הפיקוח החל ב- 40 גופים המשתייכים למגזר בתי אבות והוסטלים, שנבחרו על ידי הרשות. בסופו של יום, השיבו 31 גופים לשאלוני הפיקוח (לאחר שהתברר כי חלק מהגופים סיימו פעילותם, שינו את תחום פעילותם, נמצאו ככאלו שאינם עובדים עם מערכות ממוחשבות, וחלקם השיבו מענה מאוחד בשל פעילות עסקית מאוחדת ,ניהול מאגר משותף או תשתית טכנולוגית משותפת).

בסיום ההליך, בכל 31 הגופים המפוקחים נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר יישומה.

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

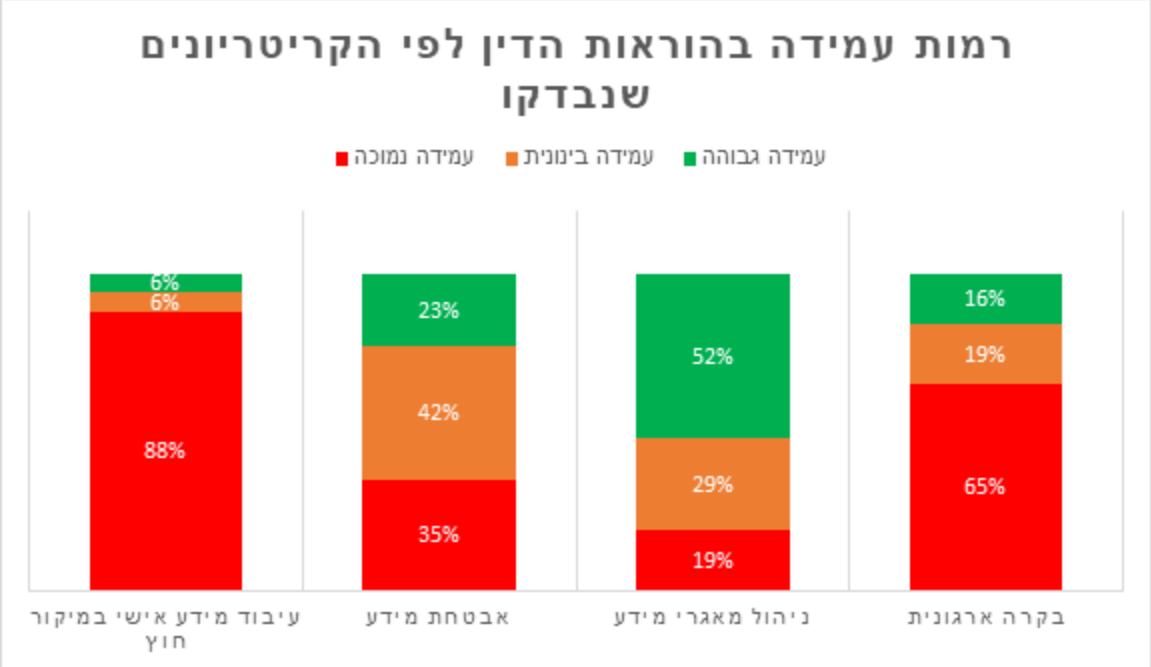
במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לארבעה קריטריונים:

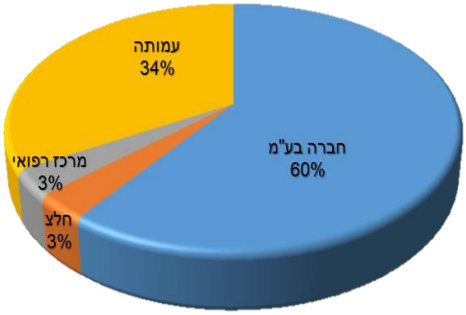
- **בקרה ארגונית** - קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות, ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע -** קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר, ואיסוף של מידע ביומטרי;
- **עיבוד מידע אישי במיקור חוץ** - 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 ובהחזקתו;

רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו בתי האבות, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:

- עמידה של בין 80% - 100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;
- עמידה של בין 60% - 80% מוגדרת כרמת עמידה בינונית או חלקית;
- עמידה של מתחת ל-60% מוגדרת כרמת עמידה נמוכה.

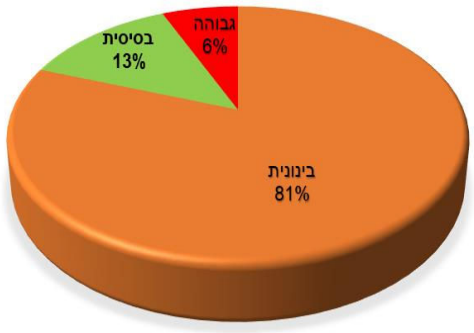
ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי





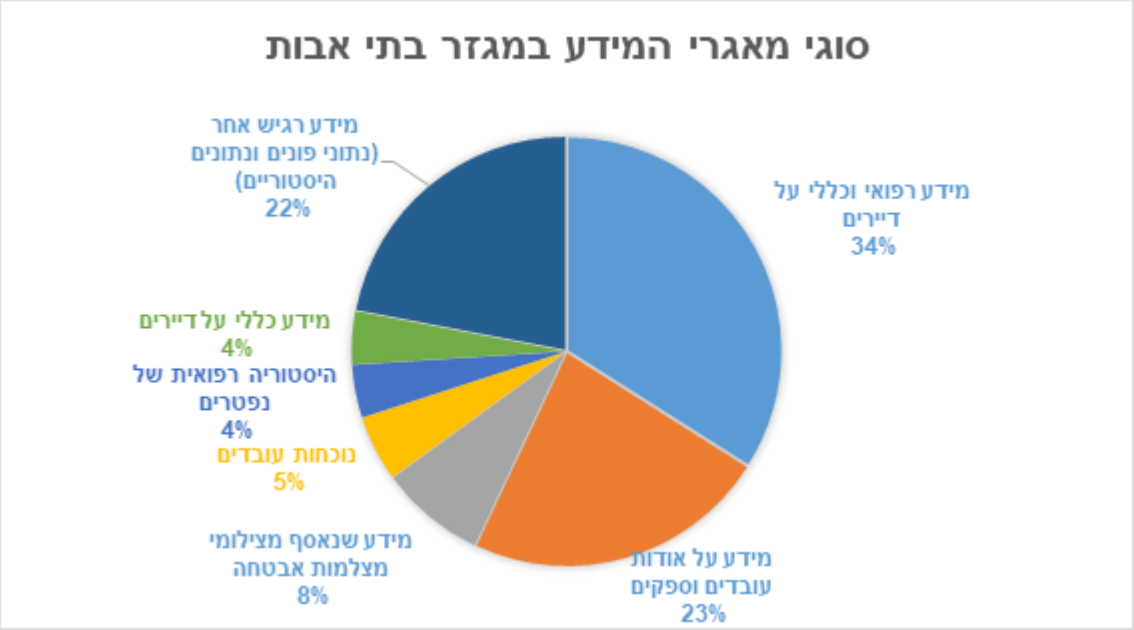
ב-31 יעדי הפיקוח שנבדקו, צורת ההתאגדות הרווחת הינה בדרך של חברה בע"מ (60%). יתר הגופים התאגדו כעמותה או כחברה לתועלת הציבור (37%). קיים גוף אחר שמאוגד כמרכז רפואי.

בחינת רמת אבטחת המידע במאגרי המידע של 31 יעדי הפיקוח שנבדקו, מצביעה כי 87% מהמאגרים מוגדרים ברמת אבטחה בינוניות וגבוהה, ו-13% בלבד מהמאגרים מוגדרים ברמת אבטחה נמוכה. סיווגם של מרבית מאגרי המידע ברמת אבטחה בינונית וגבוהה נובע מכך שקיים בהם מידע רפואי וברובם מספר בעלי ההרשאה עולה על עשרה.



בהתאם לחוק הגנת הפרטיות, במאגרים ברמת אבטחה בינונית וגבוהה, קיימת חובה, לבצע מבחני חדירות בתדירות של 18 חודשים, ולקיים בקרות נוספות.

להלן פילוח של התפלגות מאגרי המידע במגזר בתי אבות והוסטלים, לפי סוגי המידע במאגרים:

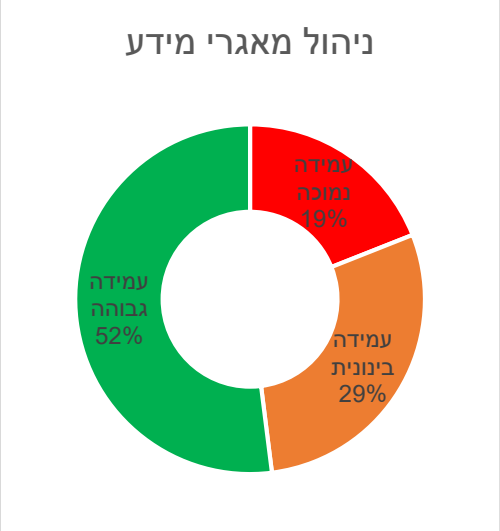


את טבלת הממצאים העיקריים שנמצאו במגזר וההנחיות שניתנו לתיקון הליקויים לגופים הספציפיים, ניתן למצוא בנספח א' להלן.

בקרה ארגונית

- במסגרת בחינת קריטריון זה, נמצא כי רק 16% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לבקרה ארגונית, בעוד ש-84% נמצאו כבעלות רמת עמידה בינונית ונמוכה בהוראות החוק כאמור.
- ב-97% מהגופים לא נמצא תיעוד מסודר לנהלי אבטחת מידע, או שהנהלים אינם מספקים כיוון שאינם מתייחסים לכלל ההיבטים הנדרשים לפי התקנות.
- ב-74% מהגופים לא נמצא תיעוד על הדרכות לעובדים בעלי גישה למאגרי מידע או למערכות המאגר, או שתדירות ההדרכות פחותה מאחת לשנתיים או שההדרכות אינן כוללות בצורה מספקת את פירוט החובות המוטלות לפי החוק והתקנות.

ניהול מאגרי מידע



- במסגרת בחינת קריטריון זה, נמצא כי 52% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לבקרה ארגונית, בעוד ש-48% מהגופים נמצאו ברמת עמידה בינונית או נמוכה בהוראות החוק כאמור.
- 68% מהגופים אינם מקפידים על קיום הוראות סעיף 11 לחוק, המחייב להודיע לאדם שנאסף ממנו מידע אישי האם חלה עליו חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.[1]

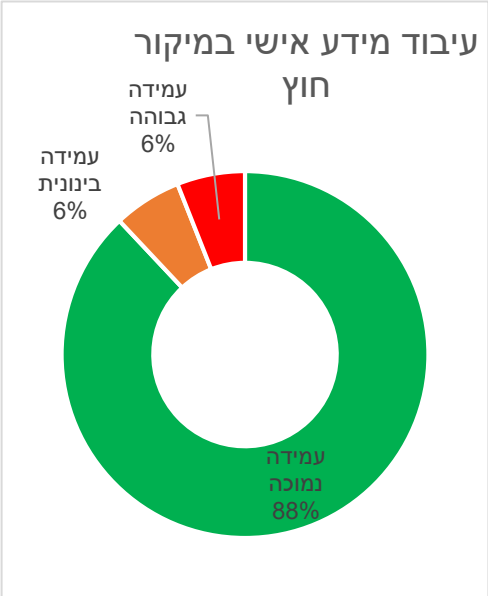
אבטחת מידע

- במסגרת בחינת קריטריון זה, נמצא כי רק 23% מהגופים עמדו ברמה גבוהה בהוראות החוק והתקנות בנוגע לקריטריון אבטחת המידע, בעוד ש-77% נמצאו ברמת עמידה בינונית או נמוכה בהוראות החוק והתקנות כאמור.
- ב-84% מהגופים לא גובש נוהל עבודה סדור לטיפול באירועי אבטחת מידע כנדרש בתקנה 11(ב) לתקנות אבטחת מידע.
- ב-74% מהגופים נמצאו ליקויים רבים בנושא אבטחת אמצעים נתיקים, כנדרש בתקנה 12 לתקנות, בין אם בהעדר הגבלות על שימוש באמצעים אלו, או בהעדר הצפנה נאותה.
- ב-81% מהגופים שמאגר המידע שלהם מוגדר ברמת אבטחת מידע בינונית ומעלה לא קוימו הוראות התקנות בנוגע לזיהוי ואימות בעלי הרשאה. כך, לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לדרישת תקנה 9(ב)(1), ולא קוים מנגנון הרשאות גישה המבוסס על הצורך לדעת התואם לכל תפקיד במידה הנדרשת לביצוע אותו תפקיד.
- ב-74% מהגופים שנבדקו לא נקבע בנוהל האבטחה אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה, הכוללת בין היתר שימוש בסיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכדומה, כנדרש בתקנה 9(ב)(2) בתקנות.

[1] להרחבה בנוגע לחובת היידוע לפי סעיף 11 לחוק הגנת הפרטיות, ראו מסמך בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (יולי 2022). המסמך זמין כאן.

- ב-78% מהגופים לא קוים מנגנון לתיעוד מלא עבור הגישה למערכות המידע או שלא נמסר מידע בנושא כנדרש בתקנה 10 לתקנות.
- ב-81% מהגופים לא קיים תהליך סדור לגיבוי לוג נתוני אבטחת מידע עבור נתוני מאגר המידע כנדרש בתקנה 17 לתקנות.
- במרבית הארגונים שנבדקו לא נמצא תיעוד לעריכת בחינה האם המידע הנשמר במאגר רב מן הנדרש למטרות המאגר, דהיינו האם הגוף מחזיק מידע עודף שאינו נחוץ לו עוד, כנדרש לפי תקנה 2(ג). בחינה זו, שהדין מחייב לערוך אחת לשנה לכל הפחות, משמעותית בכל הקשור לשמירת מידע על נפטרים כחלק ממדיניות צמצום מידע עודף, שאינו נדרש עוד למטרות המאגר בו הוא שמור אלה.[2]

עיבוד מידע אישי במיקור חוץ



- חלק זה נבדק ביחס ל-17 מתוך 31 המפוקחים, אשר דיווחו על הסתייעות בגורם חיצוני לעיבוד מידע אישי.
- במסגרת בחינת קריטריון זה, נמצא כי רק 6% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לעיבוד מידע אישי במיקור חוץ, בעוד ש-94% נמצאו ברמת עמידה בינונית ונמוכה בהוראות החוק כאמור.
- ב-88% מגופים אשר ביצעו התקשרות עם ספקי מיקור חוץ, לא בוצעו כלל הפעולות הנדרשות בהתאם לתקנה 15, לא יושמה הנחיית רשם מאגרי המידע מס' 2/2011 (שימוש בשירותי מיקור חוץ לעיבוד מידע אישי). בכלל זה, נמצא כי בתי אבות והוסטלים רבים לא נקטו באמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, או שלא נכללו התייחסויות במסמך ההתקשרות לחובותיו ואחריותו של הספק, בניגוד להוראות התקנות.

מסקנות/תמונת מצב והמלצות:

בקרה ארגונית

[2] להרחבה ראו מסמך המדיניות של הרשות להגנת הפרטיות בנושא צמצום מידע (2021). המסמך זמין כאן.

- כחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, תוך התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.[3]
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתבי מינוי רשמיים למנהל המאגר ולממונה אבטחת המידע היכן שמינויו נדרש, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, על הארגונים לגבש נוהל אבטחת מידע ולבחון את הצורך לעדכנו אחת לשנה, כנדרש בתקנות (תקנה 4).
- בהתאם להוראות התקנות, יש לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם יקבלו גישה למאגר המידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה זו לפחות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. יש לשמור את תיעוד החומרים שהועברו וכן התיעוד לביצוע ההדרכות.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או בעלי הרשאת גישה אחרים למאגר המידע, על מנת לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגרים. זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

ניהול מאגרי מידע

- יש ליידע את נושא המידע בדבר מקור הסמכות לאיסוף המידע על אודותיו. אם לא קיים מקור סמכות בחוק, יש לקבל את הסכמתו עבור איסוף המידע ושמירת פרטיו במאגרי המידע. זאת, תוך מתן הודעה בעת איסוף המידע, 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, בהתאם להוראת סעיף 11 לחוק.[4]

אבטחת מידע

[3] לקריאה נוספת על רישום מאגר מידע ומטרותיו ראו פירוט באתר הרשות להגנת הפרטיות:
https://www.gov.il/he/Departments/Guides/registration_fqa
[4] להרחבה ראו עמדת הרשות להגנת הפרטיות בנושא "חובת יידוע במסגרת איסוף ושימוש במידע אישי", לעיל ה"ש 1.

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת בתקנות. בעניין זה על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשה במידע הנ"ל. **בעניין זה, עמדת הרשות היא כי רמת אבטחת המידע הנדרשת של מאגרי המידע לא משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הינו סך כל בעלי ההרשאה לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.**
- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות. בנוסף, נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע. במאגרי מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמת אבטחה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.
- 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 שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 6 חודשים. כמו כן יש לעגן את מדיניות הסיסמאות בנוהל עבודה כנדרש בתקנה 9(ב) לתקנות.
- על הארגון לנהל מנגנון תיעוד אוטומטי, שיאפשר ביקורת על הגישה למערכות המאגר ויכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה, כנדרש בתקנה 10. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
- בנוסף, על בעל מאגר המידע לקבוע נוהל בדיקה שגרתי עבור נתוני התיעוד של מנגנון הבקרה.

- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, ולקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר, באופן שיבטיח כי ניתן יהיה, לשחזר בכל עת את הנתונים האמורים למצבם המקורי, כנדרש בתקנה 17 ותקנה 18 לתקנות.

בהתאם לתקנה 2(ג) לתקנות אבטחת מידע, על הגופים לערוך, לפחות אחת לשנה, בחינה האם קיים במאגר מידע עודף, רב מן הנדרש למטרות המאגר, ולתעד בחינה זו. בין היתר, יש לבחון האם מצוי במאגר מידע עודף בנוגע לדיירים שעזבו או שנפטרו, ששוב אינו נדרש עוד למטרות המאגר.[5]

1.4. עיבוד מידע אישי במיקור חוץ

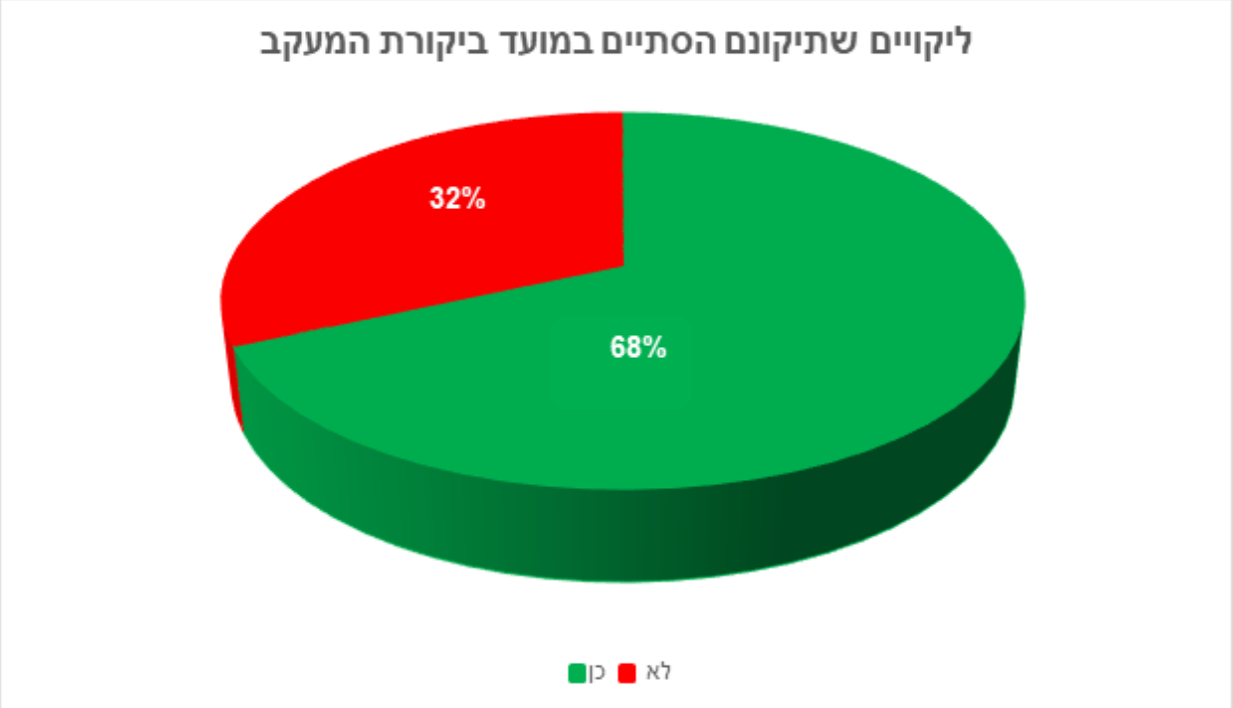
- בהתאם לתקנה 15 לתקנות אבטחת מידע, על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הרכיבים המנויים בתקנה 15(א)(2) לתקנות, לרבות חובתו של הגורם 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.[6]

שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2020, נערך מעקב תיקון ליקויים במגזר בתי אבות והוסטלים, במסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בנוסף, בוצעו על ידי הרשות להגנת הפרטיות, פיקוחי מעקב מדגמיים על חלק מהגופים בהם נמצאו ליקויים. ההחלטה על קיום פיקוח המעקב בגופים מסוימים התקבלה לאחר שנלקחה בחשבון כמות הליקויים, מהותם של הליקויים, והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישותיה. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים, ואת העמידה בלוחות הזמנים שהגדירו ליישום התכנית ותיקון יתרת הליקויים שטרם תוקנו.

[5] להרחבה ראו מסמך המדיניות של הרשות להגנת הפרטיות בנושא צמצום מידע עודף (2021). המסמך זמין כאן.
[6] 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.

במסגרת ביקורת המעקב שנעשתה בקרב 29% מהגופים במגזר בתי האבות וההוסטלים שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שנכללו בביקורת המעקב שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי.



לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע לביצוע הליכי אכיפה משלימים, לרבות בכל הנוגע למסירת תכניות העבודה לתיקון הליקויים וליישומן.

פיקוחי המעקב שבוצעו במגזר בתי האבות וההוסטלים מעידים באופן חד משמעי על כך שעצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרוחב.

2. סיכום

כאמור, מגזר בתי אבות והוסטלים הינו בעל מאפיינים ייחודיים בהיבטי פרטיות, הבאים לידי ביטוי בין היתר בהחזקה וניהול של מידע רגיש על מצבם הבריאותי של הדיירים, שימוש בשירותי מיקור חוץ, ופערי כוחות משמעותיים בין בעלי המאגרים לבין הדיירים. ממצאי הליך פיקוח הרוחב העלו ממצאים מדאיגים בתחום הבקרה הארגונית, אבטחת המידע ועיבוד מידע אישי במיקור חוץ. ניכר, כי מגזר בתי האבות וההוסטלים אינו מכיר בצורה מספקת את דרישות החוק ותקנות אבטחת מידע, וכפועל יוצא אינו עומד בהן. כמו כן, מרבית הגופים לא עמדו בהוראות החוק ותקנות אבטחת מידע ביחס לעיבוד מידע אישי בעת הסתייעות בגורם חיצוני.

כמו כן, ממצאי הליך פיקוח הרוחב עולה כי לא גובשו הנחיות בדבר צמצום מידע עודף על דיירים שנפטרו או שעזבו, שאינו דרוש עוד למטרות המאגר, כמתחייב גם בתקנה 2(ג) לתקנות.[7]

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הגופים שנבדקו תהליך בחינה והנעה לשיפור אופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית עבודה לתיקון הליקויים.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי מאגרי מידע והמחזיקים בהם באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים שהונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על הזכות החוקתית לפרטיות.

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

[7] ראו ה"ש 5

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

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית וממשל תאגידי			
לא בוצעו 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**
לא קיים נוהל אבטחת מידע או שנוהל אבטחת המידע כולל פחות מ- 50% מהסעיפים המפורטים בתקנות.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכונה בהתאם לנוהל.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4.	**נהלי אבטחת מידע**
לא מונה מנהל מאגר.	יש למנות מנהל מאגר מידע, ולעדכן את הרשות להגנת הפרטיות בהתאם.	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות.	**מינוי מנהל מאגר**
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**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
אבטחת מידע			
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**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
קיימת אפשרות לחבר התקנים ניידים ואין הצפנה.	הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 12	**התקנים ניידים והצפנה**
העברת מידע מכל מאגרי המידע ברשת ציבורית או האינטרנט אינה נעשית באמצעות שימוש בשיטות הצפנה מקובלות	בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, תקנה 14(ב), העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב)	**העברת מידע בין מאגרים**
לא קיים תיעוד של אירועי אבטחה.	יש לתעד כל אירוע המעלה חשש לאירוע אבטחה. בנוסף, על נוהל העבודה לכלול 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 מנוהל מנגנון תיעוד אוטומטי שמאפשר 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 הניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.	בקרה ותיעוד גישה תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 10.	**גישה מרחוק**
בכניסה למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב-1).	**שימוש באמצעי פיזי מרחוק**
לא קיימים אמצעי הגנה מספקים אשר נותנים מענה לחדירה לא מורשית במאגרי המידע מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישה בתקנות.	יש לוודא 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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (א).	**אבטחת תקשורת**
לא קיימת הפרדה ברורה בין המאגרים הכוללים מידע אישי לבין יתר המאגרים.	יש לקיים הפרדה בין מערכות המאגר אשר מהן ניתן לגשת למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	ניהול מאובטח ומעודכן של מערכות המאגר תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 13 (ב).	**הפרדת מאגרים עם מידע שונה**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
ניהול מאגרי מידע			
לא ניתנת הודעה בהתאם לדרישות סעיף 11 לחוק.	מתן הודעה ללקוח בעת איסוף המידע. על נוסח ההודעה לכלול את כל רכיבי סעיף 11 לחוק, ובכלל זה 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.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11.	**מתן הודעה לנושא המידע**
אין התאמה בין המאגרים המנוהלים לבין רישומם בפנקס המאגרים.	יש לפעול להסדרת רישום מאגרי המידע בפנקס המאגרים.	חוק הגנת הפרטיות תשמ"א – 1981, סעיף 8	**רישום המאגר אצל רשם**
לא ניתן לנושא המידע לעיין במידע על אודותיו כנדרש בסעיף 13 לחוק, או שניתנה לו אפשרות לעיין באופן חלקי בלבד	יש לאפשר לנושא המידע, לבא-כוחו שהרשהו בכתב או על ידי אפוטרופסו לעיין במידע שעליו המוחזק במאגר המידע.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13	**עיון במידע**
לא ניתנת לנושא המידע האפשרות לפנות בבקשה לתקן או למחוק את המידע אודותיו לפי סעיף 14 לחוק	יש לאפשר לדייר לתקן את המידע המוחזק בעניינו, אם נמצא כי המידע אינו נכון, שלם, ברור או מעודכן.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 14	**שינוי/תיקון המידע**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
עיבוד מידע אישי במיקור 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 ננקטות פעולות לוודא כי הגורם החיצוני נוקט באמצעים הנדרשים בכדי להגן על מאגרי המידע כנדרש.	יש לוודא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע, 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**