

# דו"ח פיקוח רוחב

## 2018-2019

ממצאי הליך פיקוח הרוחב –  
הגנת הפרטיות בקרב מכונים רפואיים ומעבדות  
רפואיות



אייר תש"פ  
מאי 2020



## תוכן עניינים 1

|    |                                                                                       |
|----|---------------------------------------------------------------------------------------|
| 3  | 1. תקציר מנהלים                                                                       |
| 3  | 1.1 פיקוחים מגזריים                                                                   |
| 3  | 1.2 מגזר מכונים ומעבדות רפואיות                                                       |
| 4  | 1.3 תהליך העבודה                                                                      |
| 4  | 1.4 ליקויים, מסקנות והמלצות עיקריות                                                   |
| 6  | 2. מכונים ומעבדות רפואיות - תמונת מצב                                                 |
| 6  | 2.1 כללי                                                                              |
| 6  | 2.2 רקע על המגזר                                                                      |
| 8  | 2.3 תהליך העבודה                                                                      |
| 8  | 2.4 הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו |
| 9  | 3. ממצאים – ליקויים מרכזיים                                                           |
| 9  | 3.1 בקרה ארגונית וממשל תאגידי                                                         |
| 10 | 3.2 ניהול מאגרי מידע                                                                  |
| 10 | 3.3 אבטחת המידע                                                                       |
| 11 | 3.4 עיבוד מידע אישי במיקור חוץ                                                        |
| 11 | 4. מסקנות/תמונת מצב והמלצות                                                           |
| 11 | 4.1 בקרה ארגונית וממשל תאגידי                                                         |
| 12 | 4.2 ניהול מאגרי מידע                                                                  |
| 12 | 4.3 אבטחת מידע                                                                        |
| 13 | 4.4 עיבוד מידע אישי במיקור חוץ                                                        |
| 14 | 5. סיכום                                                                              |
| 15 | נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם                            |

## 1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות ("הרשות") מופקד על עריכת פיקוחי רוחב מגזריים או נושאים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות" או "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות הגנת הפרטיות" אבטחת מידע"), במטרה לאתר הפרות של החוק, להגברת מודעות המשק להוראות החוק, להגברת האכיפה היוזמת של הרשות, לאיתור כשלים ענפיים הדורשים התייחסות והבהרות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות החוק.

### 1.1 פיקוחים מגזריים

במסגרת הליך פיקוח הרוחב ביצעה הרשות 233 הליכי פיקוח רוחב, לבדיקת היבטי הגנת הפרטיות ואבטחת המידע בקרב 9 המגזרים הבאים: 30 מרפאות לבריאות הנפש, 23 מכונים ומעבדות רפואיות, 54 חברות המנהלות מאגרי מידע של מועדוני לקוחות בהיקפים של למעלה ממאה אלף איש, 38 גופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים ו-36 חברות המספקות שירותי אחסון ועיבוד מאגרי מידע. בנוסף, הרשות ערכה 54 פיקוחי רוחב ייעודיים לבדיקת רמת אבטחת המידע במגזרי התיירות, בעמותות ואיגודים, מוסדות חינוך ובחברות טכנולוגיה המספקות שירותים טכנולוגיים בתחומי הבחירות.

דו"ח זה מפרט את הליך פיקוח הרוחב במגזר מכונים רפואיים, על אתגריו המיוחדים ומסקנותיו המגזריות.<sup>1</sup>

### 1.2 מגזר מכונים ומעבדות רפואיות

הרשות להגנת הפרטיות הגדירה את מגזר מכונים ומעבדות רפואיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה, הכוללים, בין היתר, את אופי היחסים בין הגוף המטפל והמטופל, במסגרתם נדרש למסור מידע אודות מצבו הבריאותי, או שמידע כאמור נאסף תוך כדי הטיפול ובמסגרתו מידע אודות מצבו הבריאותי של אדם מוגדר בחוק כמידע רגיש. במסגרת הגופים שנבדקו, מדובר, בין היתר, במידע רפואי דוגמת אבחוני שמיעה, קלינאות תקשורת, הדמיה ופיזיותרפיה, פוריות, ממוגרפיה, דיאליזה, התפתחות הילד ומידע אודות מצב נפשי. כאשר במסגרת יחסים אלו המטופל אינו תמיד מודע לאופן השימוש במידע זה ולהעברתו לגורמים אחרים. בנוסף, ניהול ואחזקת המידע אודות מצבם הבריאותי של המטופלים במגזר זה מבוצע באופנים שונים כגון ניהול המידע באופן ישיר, באמצעות מיקור חוץ, או באופן ישיר ובאמצעות מאגרי קופות החולים, בהיקפי מידע גדולים וברמת רגישות גבוהה.

מהפיקוח עולה, כי הגופים הפועלים במגזר שונים זה מזה בפרמטרים שונים, לרבות שוני באופי השירותים הניתנים למטופלים, היקפי המידע במאגרי המידע שהגופים מחזיקים ומנהלים, מספר המאגרים בהם הם מחזיקים, ברמת מערכות המחשוב וביכולות ניהול ואבטחת המידע וכיוצא"ב. שוני זה לרבות היקפי ורגישות המידע הנשמר, וניהול הקשר עם

<sup>1</sup> לדוחות מסכמים נוספים על מגזרים בהם בוצע פיקוח רוחב ר' פעילות פיקוח הרוחב במחלקת האכיפה באתר הרשות להגנת הפרטיות: [https://www.gov.il/he/departments/general/enforcement\\_supervision](https://www.gov.il/he/departments/general/enforcement_supervision)

המטופלים באמצעות דיור ישיר כחלק מהשירות או לאחריו, דורש בחינה והתאמה לפרמטרים הקבועים בדין בכלל הגופים המנהלים מידע רפואי, ומחייב את אותם גופים לעמוד בדרישות חוק הגנת הפרטיות, לרבות דרישות אבטחת המידע, קיום חובת השקיפות אל מול המטופלים, וכן לעמוד בהוראות החוק בכל הנוגע לדיור ישיר ולשירותי דיור ישיר.

### 1.3. תהליך העבודה

כחלק מפעילות הליך פיקוח הרחב הרשות פנתה בדרישה למילוי שאלוני ביקורת ל-23 גופים המנהלים מכוני רפואיים.

שאלוני הביקורת בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית וממשל תאגידי, 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.

### 1.4. ליקויים, מסקנות והמלצות עיקריות

במגזר מכוני ומעבדות רפואיות נמצאו פערים משמעותיים ברמות עמידה בהוראות החוק והתקנות בקרב מכוני רפואיים גדולים או כאלו המשויכים לבתי חולים וקופות חולים, לבין מכוני רפואיים בינוניים וקטנים. כך לדוגמה, נמצא כי מרבית המכוני הרפואיים הגדולים מקיימים מסגרות ממוסדות של ממשל תאגידי בהיבטים של מינוי גורמים בעלי אחריות בתחום וניהול אבטחת מידע, ורמת מודעותם לתקנות הגנת הפרטיות אבטחת מידע ובהתאמה עמידתם בהן, הינה גבוהה, כשלעומתם במכוני רפואיים קטנים, גם אם מחזיקים מידע רב, רמת המודעות ומכאן גם העמידה בהוראות התקנות נמוכה. מהליך פיקוח הרחב עולה, כי הליקויים שנמצאו מעלים חשש לדליפת מידע דרך העברת המידע לגופים שלישיים, כגון ספקי מיקור החוץ או עובדי המכוני או מוסדות אחרים בעלי נגישות שוטפת למידע הרפואי במאגרי המידע של המרפאות. על אף רמת העמידה הגבוהה יחסית בקרב המכוני הרפואיים הגדולים? בהוראות חוק הגנת הפרטיות ובתקנות, נמצאו רמות עמידה נמוכות יחסית בקריטריון הבוחן את אופן עיבוד המידע האישי במיקור חוץ.

נוכח הממצאים שעלו מהליך פיקוח הרחב, קיבלו כלל הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם, כאשר אחד הגופים המפוקחים סיים את פעילותו, קיבל הנחיות מתאימות בנוגע לאופן מחיקת רישום מאגר המידע שברשותו. לאור בחינת הליקויים שנתגלו במגזר זה, הרשות להגנת הפרטיות רואה חשיבות בפרסום דו"ח זה, על מנת שיהווה כלי עבודה מנחה, ויאפשר לגופים נוספים המנהלים מידע רפואי לבצע הערכה עצמית ואף יגביר את המודעות לדרישות חוק הגנת הפרטיות בקרב גופים אלה. כך יוכלו הגופים בתחום לנהל את המידע של מטופליהם בצורה מיטבית, תוך שמירה על זכויותיהם והגנה על פרטיותם.

# דו"ח פיקוח רוחב 2018-2019

ממצאי הליך פיקוח הרוחב בקרב מכונים רפואיים ומעבדות רפואיות

אדר תש"פ מרץ 2020



יחסים ייחודיים בין הגוף המטפל לבין המטופל, המוסר מידע אודות מצבו הבריאותי מבלי שהוא תמיד מודע לאופן השימוש במידע שמסר ולאפשרות העברתו לגורמים אחרים



ניהול והחזקת כמות גדולות של מידע רפואי רגיש בידי גופים פרטיים

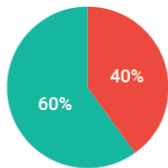


הבדלים גדולים ברמת הטיפול בנושאי אבטחת מידע בין מכונים גדולים ובינוניים לבין מכונים קטנים

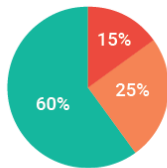
אתגרים ומאפיינים ייחודיים של מגזר המכונים והמעבדות הרפואיות



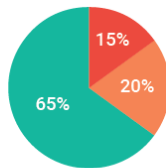
התהליך שבוצע במספרים



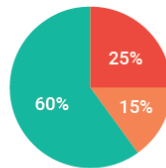
עיבוד מידע אישי במיקור חוץ



אבטחת מידע



ניהול מאגרי המידע



בקרה ארגונית וממשל תאגידי

ממצאי מכונים ומעבדות רפואיות

רמת עמידה גבוהה  
רמת עמידה בינונית/חלקית  
רמת עמידה נמוכה

אם חלה חובה למנות ממונה על אבטחת מידע, ככלל עליו להיות כפוף ישירות למנהל מאגר המידע.

מינוי מנהל למאגר המידע ועדכון רשם מאגרי המידע.

בניית תכנית עבודה שנתית לבקרה שוטפת בנושאי אבטחת מידע והגנת הפרטיות.

קביעת נוהל אבטחת מידע שיוכלל התייחסות, בין היתר, לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכד'.

שמירת המערכות במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו.

התקנת אמצעים מתאימים להגנה מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגנום נתק או שיבוש למחשב או לחומר מחשב במאגר המידע המחברים לרשת האינטרנט או לרשת ציבורית אחרת.

ניהול מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכלול את זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליזו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללונג אבטחת מידע וקביעת נהלים וביצוע גיבויים ללונג נתוני האבטחה במאגר באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים למצבם המקורי. נתוני התיעוד יישמרו למשך 24 חודשים לפחות.

במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנהל.

מתן הודעה לאדם עליו נאסף המידע בעת איסופו בה יצוין האם חלה על אותו אדם חובה חוקית למסור את המידע, או לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

יש לאפשר לאדם לעדכן את המידע אודותיו שאינו נכון/שלם/ברור או מעודכן.

ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לקבוע בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) עבור כל צד שלישי אשר מספק שירותי עיבוד מידע אישי לחברה.

מסמך ההתקשרות עם גורם חיצוני בעל גישה לאתר צריך לכלול התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות לרבות דיווח אודות אירועי אבטחת מידע, מנגנוני אבטחת מידע, שמירת המידע לאחר סיום תקופת ההתקשרות וחובות צד שלישי בהעברת מידע לאחר.

לודא כי כל צד שלישי אשר מספק שירותי מיקור חוץ בתחום מאגרי המידע נקט באמצעים הנדרשים בהוראת ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.

## 2. מכונים ומעבדות רפואיות - תמונת מצב

### 2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2018 לאוגוסט 2019 במגזר מכונים ומעבדות רפואיות.

### 2.2. רקע על המגזר

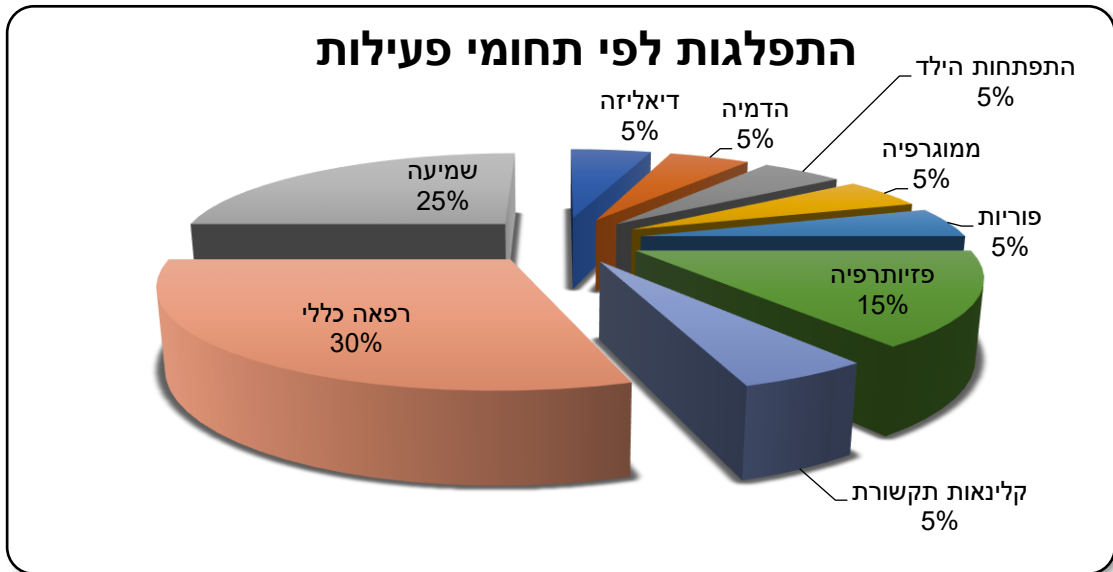
במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר המכונים הרפואיים כיעד פיקוח רחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר. מאפיינים אלו כוללים, בין היתר, את היחסים בין הגוף המטפל והמטופל, במסגרתם נדרש למסור מידע אודות מצבו הבריאותי, או שמידע כאמור נאסף תוך כדי הטיפול ובמסגרתו. כאשר במסגרת יחסים אלו המטופל אינו תמיד מודע לאופן השימוש במידע זה ולהעברתו לגורמים אחרים. בנוסף, ניהול ואחזקת המידע אודות מצבם הבריאותי של המטופלים במגזר זה מבוצע באופנים שונים כגון ניהול המידע באופן ישיר, באמצעות מיקור חוץ, או באופן ישיר באמצעות מאגרי קופות החולים, בהיקפים גדולים וברמת רגישות גבוהה.

למגזר זה ייחודיות באופי המידע הנשמר, הקבוע בחוק הגנת הפרטיות כמידע רגיש, הכולל כחלק מהשירותים הניתנים, מעבר לנתונים הכלליים אודות המטופלים כגון מידע אישי ודמוגרפי, גם מידע רפואי על גווניו - וכפי שנמצא בגופים שנבדקו גם מידע אודות אבחוני שמיעה, קלינאות תקשורת, הדמיה ופיזיותרפיה, וכן מידע רפואי על פוריות, ממוגרפיה, דיאליזה, התפתחות הילד ומידע נפשי.

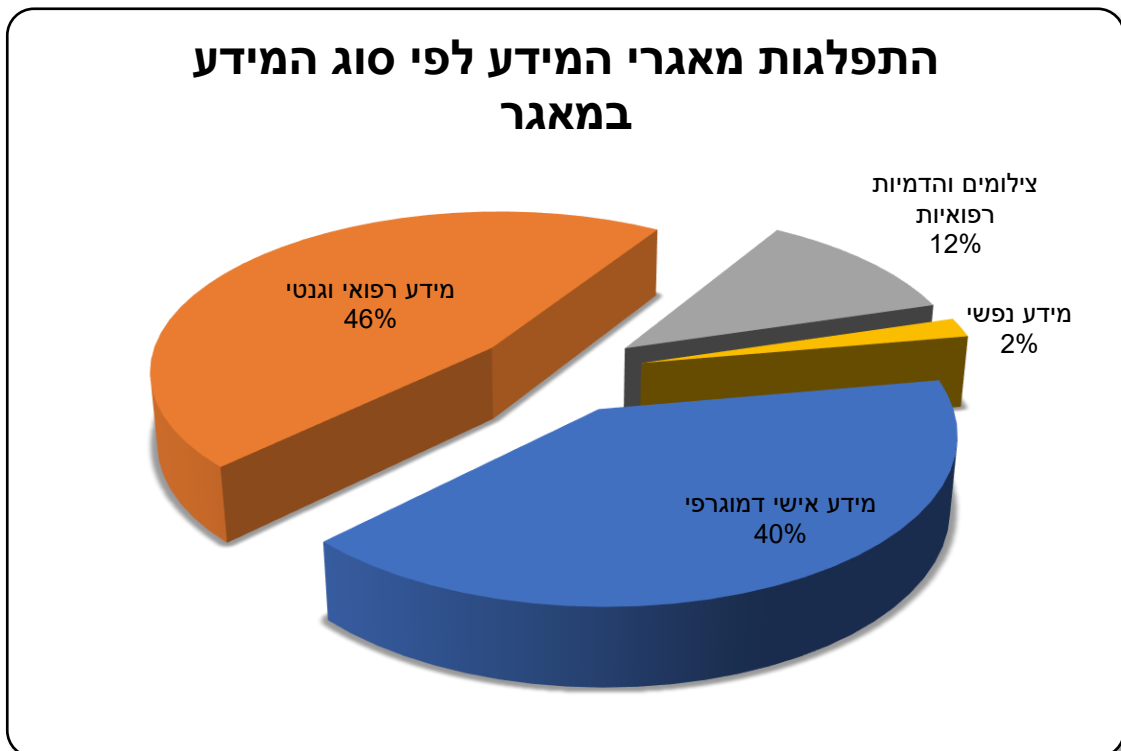
הגופים הפועלים במגזר זה הם בעלי שונות רבה באופי ובגודל הגופים, במספר המאגרים (10% מהגופים מנהלים למעלה מ-5 מאגרי מידע, כ-55% מהגופים מנהלים בין 2-5 מאגרים וכ-35% מהגופים מנהלים מאגר מידע אחד), במערכות המחשוב וביכולות ניהול ואבטחת המידע - החל מגופים בעלי עשרות סניפים, ועד לגופים פרטיים קטנים בעלי מערכות מחשוב בודדות. הדורשת בחינה והבהרה אחידה לגבי אופן ניהול המידע בהתאם להוראות הדין.

סוג המידע הנשמר, היקפיו, רגישותו וניהול הקשר עם המטופלים באמצעות דיורר ישיר כחלק מהשירות או לאחריו, מחייב את אותם גופים לעמוד בדרישות אבטחת המידע, לקיים את חובת השקיפות אל מול המטופלים, ולעמוד בהוראות החוק בכל הנוגע לדיורר ישיר ולשירותי דיורר ישיר.

**התפלגות פעילות כלל הגופים המפוקחים, לפי תחומי פעילותם**



**התפלגות מאגרי המידע לפי סוג המידע במאגר**



## 2.3. תהליך העבודה

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בשלב של בניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לתחומים בסיכון מוגבר לפרטיות שזיהתה הרשות כמפורט ברקע על המגזר, ולמדיניות השנתית של הרשות. התכנית נבנית בהתחשב בגורמים הבוחנים את כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר/נושא, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

כחלק מבחירת הגופים המפוקחים במגזר המכונים והמעבדות הרפואיות, בחרה הרשות 23 גופים המנהלים סניפים בהיקפים שונים (החל מגופים קטנים המנהלים סניפים אחדים ועד לגופים המנהלים עשרות סניפים), המספקים שירות לכמה קופות חולים, וסה"כ נבחרו גופים המנהלים יחדיו כ-309 מכונים בפריסה גיאוגרפית כלל ארצית, הכוללים מידע רפואי על היקף גדול של נושאי מידע.

השאלונים נשלחו ל- 23 גופים המנהלים מכונים רפואיים, כאשר בניכוי גופים אשר סיימו פעילותם, שינו פעילות, דיווחו על פעילות שאינה רלוונטית למגזר זה, נבדקו במסגרת הליך הפיקוח 20 גופים. במסגרת התהליך 4 גופים מתוכם נדרשו לספק מידע, מסמכים, והבהרות נוספות לרשות, כאשר באחד מאותם הגופים הושלמו ואומתו ידיעות ומסמכים באמצעות פיקוח במשרדי הגוף המפוקח. אחד הגופים המפוקחים אשר סיים את פעילותו, קיבל הנחיות מתאימות בנוגע לאופן מחיקת רישום מאגר המידע שברשותו. בסיום ההליך, נמצאו ב-20 הגופים שנבדקו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את אותם 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.

## 2.4. 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, הבוחנים זאת על בסיס קריטריונים שונים ובהם:

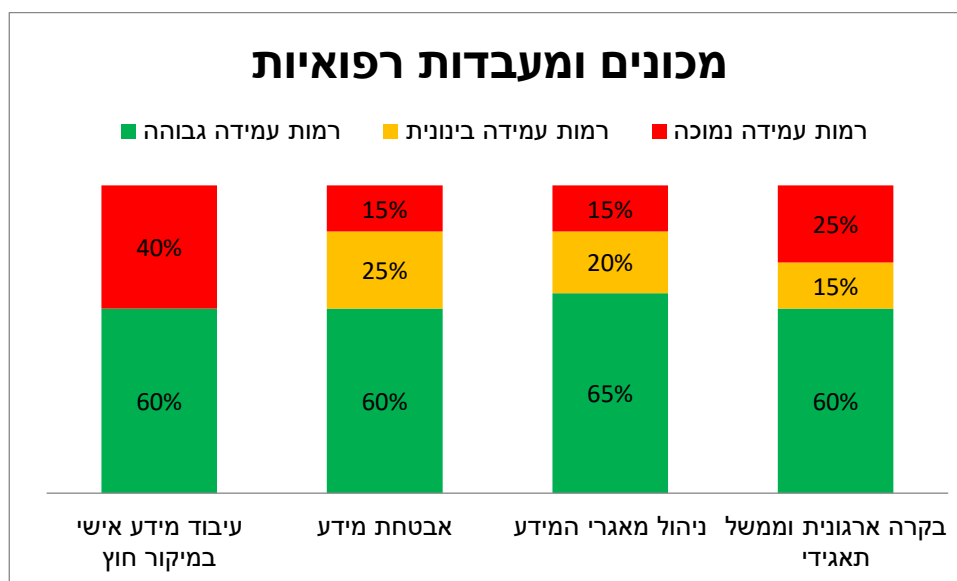
- **בקרה ארגונית וממשל תאגידי** - קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** – קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר;
- **אבטחת מידע** - בחינת עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם;
- **שירותי מיקור חוץ** - בחינת ההתקשרויות של בעלי מאגרי המידע עם גורמים שלישיים המחזיקים במידע ומעבדים אותו והאופן בו הם מבטיחים הגנה על המידע.



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

- 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.

### 3. ממצאים – ליקויים מרכזיים



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

#### 3.1 בקרה ארגונית וממשל תאגידי

- במרבית הגופים (60%) נמצאה רמת עמידה גבוהה יחסית בהוראות החוק בנוגע לבקרה הארגונית וממשל תאגידי.<sup>2</sup>
- ב-40% מהגופים בהם נמצאה רמת עמידה בינונית ומטה בדרישות הממשל התאגידי, נמצאו ליקויים בהגדרת מאגר המידע ומטרותיו ואי מילוי הדרישה למינוי של מנהלי מאגרים. גם כאשר מונו כאלו, נמצאו גופים מפקחים אשר מינו בעלי תפקידים ללא כתב מינוי ועדכון בפנקס מאגרי המידע כנדרש.
- נמצאו פערים בנושא ביצוע בדיקת התאמה לעובדים חדשים בעלי גישה למאגר כדי לברר שאין חשש כי בעל הרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר.

<sup>2</sup> עמידה גבוהה זו מיוחסת בחלקה לדרישות המוטלות על גופים הפועלים במגזר זה כחלק ממערכת החובות המוטלות על ידי משרד הבריאות והרגולציה הפרטנית הנוגעת למתן שירותים רפואיים. דרישות אלו נמצאו כמקיפות באופן חלקי בלבד בהיבטי הממשל הארגוני, ניהול מאגרי המידע ואבטחת המידע, בדגש על הגופים הגדולים הפועלים במגזר זה, אך נמצאו כלא מספקות בכל הנוגע לאופן ההתקשרות של גופים אלו עם מיקור חוץ לצורכי עיבוד ואחסון המידע.

- נמצאו גופים אשר אין להם תיעוד מסודר לנהלי אבטחת מידע ולתכנית עבודה שנתית לבקרה שוטפת על העמידה בדרישות התקנות, או שהנהלים אינם מספיק איכותיים בכך שאינם מקיפים את כלל הדרישות בהוראות התקנות.
- בנוסף, נמצאו גופים בעלי מאגרי מידע שחלה עליהם רמת אבטחה גבוהה, אשר נדרשו לבצע מבדקי חדירות אשר לא ביצעו אותם כנדרש או לא ביצעו כלל.

### 3.2. ניהול מאגרי מידע

- בתחום ניהול מאגרי מידע, נמצא כי 65% מהגופים עמדו בדרישות ברמה הגבוהה (מעל 80% עמידה), 20% ברמת הבינונית (בין 50%-80%), ו-15% ברמה נמוכה (מתחת ל-50% עמידה).
- מקרב הגופים שנמצאה בהם רמת עמידה נמוכה, היו כאלו אשר כמעט ולא עמדו בדרישות החוק בכל הנוגע לרישום מאגרי המידע.
- נמצאו ליקויים ביישום הוראות החוק בכל הנוגע לשקיפות בדבר מקור הסמכות לאיסוף המידע האישי וידוע האנשים עליהם מוחזק המידע, בדבר זכויותיהם בנוגע למאגר המידע הרפואי בו נשמרים פרטיהם.
- נמצאו גופים אשר לא הבהירו לנושאי המידע את זכותם לעיין במאגרי המידע.
- נמצאו גופים אשר לא אפשרו לנושאי המידע לשנות/לתקן את המידע המוחזק אודותיהם כנדרש בחוק.

### 3.3. אבטחת המידע

- במרבית הגופים (60%) נמצאה רמת עמידה גבוהה בהוראות החוק בנוגע לאבטחת מידע.<sup>3</sup>
- נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בהעדר תהליכים נאותים לניהול הרשאות ובין אם בהעדר יישום הפרדת תפקידים ויישום מתן ההרשאה לפי עקרון הצורך לדעת בלבד (בעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות).
- נמצאו ליקויים רבים בנושא אבטחת אמצעים נתיקים בין אם בהעדר הגבלות על שימוש באמצעים אלו, או בהעדר הצפנה נאותה.
- בנוסף, נמצאו גופים אשר לא נקטו באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את ו/או המאפשרים גישה אל מאגרי המידע.
- נמצאו גופים בעלי רמת אבטחת מידע בינונית ומעלה, אשר בכניסה למאגר המידע באמצעות רשת האינטרנט, לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- כמו כן, נמצאו גופים אשר לא ביצעו מעקב ותיעוד של אירועי אבטחת מידע.
- נמצא כי בגופים מסוימים לא נקבע בנהל האבטחה נושא הניתוק האוטומטי לאחר פרק זמן של אי-פעילות.

<sup>3</sup> ר' הערת שוליים 2

### 3.4. עיבוד מידע אישי במיקור חוץ

- בין הגופים אשר דיווחו כי הם עושים שימוש במיקור חוץ לצורכי עיבוד מידע, 40% מהגופים נמצאו ברמת עמידה נמוכה.
- ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בפנים הארגון, קיים עדיין ליקוי ביישום הדרישות מחברות צד ג' המעניקות שירותי עיבוד מידע אישי במיקור חוץ.
- ליקוי זה מתבטא בכך שחלק מהגופים לא נקטו צעדים מספקים מבעוד מועד על מנת להעריך את מידת הסיכון הנשקפת למידע ולפגיעה אגב כך בזכותם לפרטיות של נושאי המידע, הנובע משימוש במיקור חוץ.
- מבין אותם גופים אשר מבצעים שימוש במיקור חוץ לעיבוד מידע ואשר נמצאה בהם רמת עמידה נמוכה בקריטריון זה, נמצא כי הם אינם מבצעים התקשרות עם ספק מיקור חוץ לפי הוראות התקנות בצורה מספקת, לא בוחנים את איכות ניהול אבטחת המידע ואופן תפעול מאגרי המידע אצל ספקי מיקור החוץ, ולא מבצעים פעולות בקרה ופיקוח נאותות על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.

### 4. מסקנות/תמונת מצב והמלצות

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

#### 4.1. בקרה ארגונית וממשל תאגידי

נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, וי קיום התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.

בנוסף, על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאות כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע היכן שנדרש למנות כזה וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע).

כמו כן, 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'. ובנוסף, לעדכן את נוהל אבטחת המידע כך שיהיה צורך בבחינת עדכניותו אחת לשנה, כנדרש בתקנות הגנת הפרטיות (תקנה 4).

כמו כן, על הגופים להכין תכנית עבודה לנושא אבטחת מידע והגנת הפרטיות לרבות התייחסות לנושא גורם אחראי ול"ז לביצוע, שתעמוד בדרישות תקנות הגנת הפרטיות

(תקנה 3 (3)). כמו כן, במידה ומדובר בגוף החייב במבדקי חדירות עליו לוודא כי אכן נעשו כאלה העומדים בדרישות תקנות הגנת הפרטיות (סעיף 16).

בנוסף, בהתאם לנדרש בתקנות הגנת הפרטיות (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או כל גורם אחר שמקבל גישה למאגר/מערכת מאגר.

#### 4.2. ניהול מאגרי מידע

החובה המוטלת מכוח החוק על הגופים המנהלים רשימות מטופלים הכוללות אפיון של נושאי המידע באופן הכולל מידע כהגדרתו בחוק, כוללת את הצורך לבצע מיפוי לכל מאגרי המידע הקיימים אצלם, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

על הגופים לקבל את הסכמת נושא המידע כנדרש בחוק עבור שמירת פרטיו במערכת הארגון, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

לעניין זה, לצד הדרישות הקבועות בסעיף 11 לחוק המפרטות את חובות מבקש המידע, נוכח היחסים הייחודיים בין מבקש המידע לבין המטופל, על הגופים האוספים מידע להקפיד על אופן השקיפות בפני המטופל בעת קבלת ההסכמה ומסירת המידע על ידו, ולהקפיד בכל פנייה בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או באמצעי אחר, המהווה פנייה בדיוור ישיר כהגדרתה בסעיף 17ג' לחוק, על ציון הפרטים המנויים בסעיף 17' - לרבות ציון כי הפניה היא בדיוור ישיר, זהותו ומענו של בעל מאגר המידע, מקור המידע, הגורמים להם נמסר המידע וכד'.<sup>4</sup>

בנוסף, על הגופים להקפיד ליידע ולאפשר 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 על ידי בתי עסק או גוף אחר הנותן שירות לציבור.<sup>5</sup> כמו כן, יש להקפיד ליידע ולאפשר לנושאי המידע לתקן/לשנות את המידע אודותיהם המוחזק במאגר מידע בהתאם לסעיף 14 לחוק.

#### 4.3. אבטחת מידע

נוכח הליקויים בנושא ניהול ההרשאות, על הגופים לוודא בניית מנגנוני הרשאות במאגרי המידע של הארגון בהתאם לתקנות 8-9 (א) שיבטיחו הפרדת סמכויות ויאפשרו גישה של העובדים בעלי הגישה למידע לנתוני המאגר, וזאת רק במידה הנדרשת לביצוע התפקיד..

<sup>4</sup> לקריאה נוספת ר' הנחיית רשם מאגרי מידע מס' 2/2017 פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר - [https://www.gov.il/BlobFolder/policy/direct\\_mail\\_2/he/direct%20mail.pdf](https://www.gov.il/BlobFolder/policy/direct_mail_2/he/direct%20mail.pdf)

<sup>5</sup> לקריאה נוספת ר' הנחיית רשם מאגרי המידע 1/2017 - תחולת הוראות חוק הגנת הפרטיות על זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי נוסף - [https://www.gov.il/BlobFolder/policy/right\\_of\\_access/he/video.pdf](https://www.gov.il/BlobFolder/policy/right_of_access/he/video.pdf)

כמו כן, נוכח הליקויים שנמצאו בנוגע לשימוש באמצעים נתיקים במגזר זה, מוצע כי הגורמים הרלוונטיים בגופים יקיימו דיון אודות הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או קיים צורך מינימאלי – עליהם להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.

בנוסף, על הגופים לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את ו/או המאפשרים גישה אל מאגרי המידע, על פי תקנות הגנת הפרטיות (תקנה 6). כמו כן, על הגוף לוודא שבכניסה לאתר מאגר המידע, נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, ולוודא קיום תיעוד עבור אירועי אבטחת מידע (תקנה 11 לתקנות). כמו כן, יש לוודא כי מתבצע ניתוק אוטומטי לאחר פרק זמן של אי-פעילות (תקנה 9(ב)).<sup>6</sup>

#### 4.4. עיבוד מידע אישי במיקור חוץ

בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות. בנוסף, על הגופים, בעלי המאגר, לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, כאשר יש לקבוע במפורש בהסכם את כל הוראות תקנה 15(א)(2) לתקנות הגנת הפרטיות (אבטחת מידע), 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.

עוד דורשות התקנות מן הגופים לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות. הוראות דומות לעניין החובות המוטלות על בעל מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.<sup>7</sup> ולעניין מידע רפואי בפרט בהנחיית רשם מאגרי מידע מס' 1/2009 תחולת החובות מכוח החוק במאגרי מידע רפואי שבשימוש קופות חולים ונותני שירותים רפואיים.<sup>8</sup>

<sup>6</sup> לקריאה נוספת ר' המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע) - [https://www.gov.il/BlobFolder/guide/data\\_security\\_guide/he/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%A9%20%D7%94%D7%9E%D7%9C%D7%90%20%D7%9C%D7%99%D7%99%D7%A9%D7%95%D7%9D%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA%20%D7%90%D7%91%D7%98%D7%97%D7%AA%20%D7%9E%D7%99%D7%93%D7%A2%20%E2%80%93PDF%20%D7%9C%D7%94%D7%93%D7%A4%D7%A1%D7%94\\_1.pdf](https://www.gov.il/BlobFolder/guide/data_security_guide/he/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%A9%20%D7%94%D7%9E%D7%9C%D7%90%20%D7%9C%D7%99%D7%99%D7%A9%D7%95%D7%9D%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA%20%D7%90%D7%91%D7%98%D7%97%D7%AA%20%D7%9E%D7%99%D7%93%D7%A2%20%E2%80%93PDF%20%D7%9C%D7%94%D7%93%D7%A4%D7%A1%D7%94_1.pdf)

<sup>7</sup> לקריאה נוספת ר' הנחיית רשם מאגרי המידע 2/2011 - שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי

<https://www.gov.il/BlobFolder/policy/outsourcing/he/%D7%94%D7%A0%D7%97%D7%99%D7%99%D7%AA%20%D7%A8%D7%A9%D7%9D%20%D7%9E%D7%90%D7%92%D7%A8%D7%99%20%D7%9E%D7%99%D7%93%D7%A2%20-%D7%A9%D7%99%D7%9E%D7%95%D7%A9%20%D7%91%D7%A9%D7%99%D7%A8%D7%95%D7%AA%D7%99%20%D7%9E%D7%99%D7%A7%D7%95%D7%A8%20%D7%97%D7%95%D7%A5%20%D7%9C%D7%A2%D7%99%D7%91%D7%95%D7%93%20%D7%9E%D7%99%D7%93%D7%A2%20%D7%90%D7%99%D7%A9%D7%99.pdf>

<sup>8</sup> לקריאה נוספת ר' הנחיית רשם מאגרי מידע מס' 1/2009 תחולת החובות מכוח החוק במאגרי מידע רפואי שבשימוש קופות חולים ונותני שירותים רפואיים - [https://www.gov.il/BlobFolder/policy/medical\\_information/he/medical\\_information.pdf](https://www.gov.il/BlobFolder/policy/medical_information/he/medical_information.pdf)



## 5. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות המטופלים שמידע אודותיהם מוחזק במכונים רפואיים. מכונים אלה מחזיקים ומנהלים מידע רב, מזהה ורגיש, וניהול הקשר עם נושאי המידע באמצעות הגופים ובאמצעות מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות חוק הגנת הפרטיות, הוראות תקנות הגנת הפרטיות (אבטחת המידע), שקיפות מול המטופל, ומילוי החובות החלות מכח פרק הדיוור הישיר ושירותי הדיוור הישיר בחוק.

ממצאי הליך פיקוח הרוחב במגזר מכונים רפואיים העלה ממצאים המצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ ופערים בעיקר בנוגע לקיום הוראות החוק בתחום נהלי אבטחה, מבדקי חדירות ותכנית עבודה שנתית. בנוסף נמצא כי חלק מהגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את ציבור המטופלים בדבר זכויותיו על פי חוק הגנת הפרטיות, הכללות בין היתר את החובה להציג את מקור המידע, הזכות לעיין במידע והזכות להימחק ממאגר המידע.

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל המפוקחים תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית מסודרת לתיקונם.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלים ומחזיקים במאגרי מידע אישי 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 זכות הציבור 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 במגזרים השונים, על ידי בחינת גופים אחרים במגזרים אלה, במועד שתקבע לאחר פרסום הדו"ח המגזרי.

## נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

| הליקוי/פער                                                                          | פעילות מתקנת נדרשת                                                                                                                                                                     | הפניה לחוק/תקנה/הנחיה                                                                      | נושא                   |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------|
| <b>בקה ארגונית וממשל תאגידי</b>                                                     |                                                                                                                                                                                        |                                                                                            |                        |
| לא בוצעה ביקורת אבטחת מידע.                                                         | עריכת ביקורות בנושא אבטחת מידע/הגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה, לחילופין במאגר ברמת אבטחה גבוהה - עריכת סקר סיכונים מידי 18 חודשים הכולל את דרישות הביקורת. | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, סעיף 16                                        | ביקורות תקופתיות       |
| עובדים חדשים לא עוברים הליך מיון/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      |
| בגוף המחויב במינוי ממונה אבטחת מידע על פי החוק, לא מונה ממונה אבטחת מידע.           | יש לפעול למינוי ממונה 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 |
| בגוף המחויב במינוי ממונה אבטחת מידע על פי החוק, אין למנות מנמ"ר כממונה אבטחת המידע. | יש למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחת הכפוף ישירות למנהל המאגר.                 | חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3    | מינוי ממונה אבטחת מידע |
| לא מונה מנהל מאגר.                                                                  | יש למנות מנהל למאגר המידע. ולעדכן את רשם מאגרי המידע בהתאם                                                                                                                             | פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות                                 | מינוי מנהל מאגר        |
| אין התאמה בין מנהל המאגר כפי שדווח על ידי החברה ומנהל המאגר כפי שמופיע ברשות.       | הסדרת רישום מנהל המאגר ברשם.                                                                                                                                                           | פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות                                 | מינוי מנהל מאגר        |
| נוהל אבטחת המידע שנקבע, אינו מכסה את כלל הסעיפים המנויים בתקנות                     | קביעת נוהל אבטחת מידע ובו מענה לכל הנושאים המנויים בתקנה 4, בהתאם לרמת האבטחה הנדרשת במאגר.                                                                                            | נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4                        | נהלי אבטחת מידע        |
| לא קיימים נהלי אבטחת מידע.                                                          | כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.                                                                                                                        | נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4                        | נהלי אבטחת מידע        |

| נושא                    | הפניה לחוק/תקנה/הנחיה                                                                | פעילות מתקנת נדרשת                                                                                                                                                                                                                                                                    | הליקוי/פער                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| נהלי אבטחת מידע         | נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4                  | בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם.                                                                                                                                                                                                                                  | לא הוגדר בנוהל אבטחת מידע הצורך לבחינת עדכניותו אחת לשנה.                                                           |
| תכנית עבודה             | תכנית עבודה לבקרה שוטפת 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 לבקרה שוטפת בנושא אבטחת מידע.                                                            |
| תכנית עבודה             | תכנית עבודה שנתית לבקרה שוטפת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3) | עדכון תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע כך שתכסה בצורה טובה את נושאי אבטחת מידע והגנה על הפרטיות ותפרט את הגורם האחראי ואבני דרך ברורים.                                                                                                                                 | תכנית העבודה השנתית לבקרה שוטפת בנושא אבטחת מידע אינה מפורטת מספיק ואיננה כוללת את כל הרכיבים הנדרשים מתוכנית עבודה |
| <b>ניהול מאגרי מידע</b> |                                                                                      |                                                                                                                                                                                                                                                                                       |                                                                                                                     |
| זכות לעיון/תיקון במידע  | חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13                                               | מתן אפשרות לנושא המידע לממש את זכותו החוקית לעיון במידע אודותיו בהתאם לסעיף 13 לחוק, בכלל מאגרי המידע                                                                                                                                                                                 | לא ניתן לנושא המידע לעיין במידע אודותיו לפי בקשתו כנדרש בסעיף 13 לחוק.                                              |
| זכות לעיון/תיקון במידע  | חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 14                                               | יש לאפשר לנושא המידע לעדכן את המידע שאינו נכון/שלם/ברור או מעודכן האגור אודותיו בכל מאגרי המידע.                                                                                                                                                                                      | לא ניתן לנושא המידע לתקן את המידע אודותיו לפי בקשתו כנדרש בסעיף 14 לחוק.                                            |
| פנייה לקבלת מידע        | סעיף 11 לחוק                                                                         | 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.                        | לא נמסרת המטופלים הודעה המפרטת לשם מה מבוקש המידע, למי יימסר המידע ומטרות המסירה.                                   |
| <b>אבטחת מידע</b>       |                                                                                      |                                                                                                                                                                                                                                                                                       |                                                                                                                     |
| 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. | לא קיימת אבטחה פיזית וסביבתית למערכות.                                                                              |
| 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.                                                                                            | לא מותקן אנטי וירוס בכל תחנה ושרת.                                                                                  |



| נושא                 | הפניה לחוק/תקנה/הנחיה                                                  | פעילות מתקנת נדרשת                                                                                                                                                                                                                                                                   | הליקוי/פער                                                                                                                                            |
|----------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| בקרה ותיעוד גישה     | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 10                 | יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכול ללול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של הניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.<br>נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות. | לא מנוהל מנגנון תיעוד אוטומטי שמאפשר ביקורת על הגישה למאגר מטופלים.                                                                                   |
| גיבוי נתוני אבטחה    | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 17 (ב) ותקנה 18    | 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 לתקנות.                                                         | לא קיים תהליך גיבוי ללוג אבטחת המידע, או לא התקבל מענה נאות לפירוט אמצעי הגיבוי הקיימים ללוג נתוני האבטחה במאגר, לכן לא ניתן להעריך את העמידה בתקנות. |
| גישה מרחוק           | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 14 (ג)             | אופן הזהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.                                                                                                                                                                         | בכניסה מרחוק למאגר ברמה הבינונית והגבוהה על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.                                  |
| הפרדה בין מאגרים     | תקנות הגנת פרטיות (אבטחת מידע) תשע"ז<br>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 בין סביבת הנתונים של המאגר לבין יתר הנתונים של הארגון.                                                                                 |
| התקנים ניידים והצפנה | התקנים ניידים<br>תקנות הגנת פרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 12 | הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.                                                                                                                                                       | קיימת אפשרות לחבר התקנים ניידים ולא קיימת הצפנה.                                                                                                      |
| העברת נתונים         | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 14 (ב)             | בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 14 (ב), העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).                                                                                                   | לא מבוצעת הצפנת מידע בהעברת נתונים ברשת.                                                                                                              |
| מדיניות סיסמאות      | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 9 (ב-2)            | 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 וכד'                                                                                      | במערכת לא מוטמעת מדיניות סיסמאות או לא קיימת מדיניות סיסמאות חזקה.                                                                                    |
| ניהול הרשאות         | תקנות הגנת פרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 8, תקנה 9 (א)       | אפיון ויישום תהליך בו מיד בעת סיום תפקיד או עזיבת עובד הארגון, הרשאותיו של העובד יבוטלו או יעודכנו בהתאם לצורך.                                                                                                                                                                      | לא קיים תהליך לביטול הרשאות לבעל הרשאה שסיים את תפקידו או מנגנון לעדכון הרשאות לבעל הרשאה שעבר לתפקיד חדש, או שאינו מתקיים בסמוך לשינוי סטטוס העובד.  |
| ניתוק אוטומטי        | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 9 (ב-2)            | ברמת אבטחה בינונית ומעלה, נדרשת הגדרת ניתוק אוטומטי במערכות מאגרי המידע לאחר פרק זמן סביר של אי פעילות במערכת                                                                                                                                                                        | אי ביצוע ניתוק אוטומטי לאחר פרק זמן או ביצוע ניתוק אוטומטי לאחר פרק זמן לא סביר של אי פעילות.                                                         |

| הליקוי/פער                                                                                                                                | פעילות מתקנת נדרשת                                                                                                                                                                                                                                                                                  | הפניה לחוק/תקנה/הנחיה                                                                                                                              | נושא               |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| אי עמידה בהוראות תקנה 11 בנוגע לתייעוד וקביעת הוראות התמודדות עם אירועי אבטחת מידע.                                                       | 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.<br>במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל. | תקנות הגנת פרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 11                                                                                              | תיעוד אירועי אבטחה |
| <b>עיבוד מידע אישי במיקור חוץ</b>                                                                                                         |                                                                                                                                                                                                                                                                                                     |                                                                                                                                                    |                    |
| אי בחינה וקביעה בהסכם מול גורם חיצוני הנותן שירותי עיבוד מידע אישי בחברה, כי הוא פועל בהתאם לתקנה 15 ולהנחיות רשם מאגרי המידע מס' 2/2011. | ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 הנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גוף צד ג' 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<br>2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי. | מיקור חוץ          |
| ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות                                                   | יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות:<br>1. דיווח אודות אירועי אבטחת מידע.<br>2. מנגנוני אבטחת המידע הנדרשים.<br>3. שמירת המידע לאחר סיום תקופת ההתקשרות.<br>4. חובות צד ג' בהעברת מידע לאחר.                                             | מיקור חוץ<br>תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 15                                                                                | מיקור חוץ          |
| אי נקיטת פעולות בכדי לוודא שצד ג' נוקט בהוראות ההסכם ובהוראות התקנות המפרטות את האמצעים הנדרשים להגנת המידע                               | ווידוא כי כל גוף צד ג' אשר נותן שירותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.                                                                                                                                           | תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז<br>2017, תקנה 15                                                                                             | מיקור חוץ          |

