משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר נותני שירותי סיוע במימוש זכויות רפואיות

אייר תשפ"א
אפריל 2021

תוכן עניינים

1. תקציר מנהלים

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

1.1. מגזר מרפאות מימוש זכויות רפואיות

במסגרת סקר רוחבי במגזרי המשק שערכה הרשות להגנת הפרטיות אשר בוחן את סיכוני הפרטיות במגזרים השונים, מגזר ארגונים (או גופים) אשר עוסקים בשירותי סיוע במימוש זכויות רפואיות בישראל אותר כאחד מיעדי פיקוח הרוחב המשמעותיים. מגזר זה המעניק שירותי סיוע במימוש זכויות רפואיות אל מול רשויות מדינה שונות עבור לקוחותיו, ובמסגרת זו מקבל לידיו מידע רב ורגיש, נחשב בעל מאפיינים ייחודיים המהווים סיכון בהיבטי הפרטיות. מאפיינים אלו באים לידי ביטוי ביחסים ייחודיים ופערי כוחות מובנים בין נותן השירות ומוסר המידע, אשר מוסר מידע רגיש לרבות מידע אודות מצבו הבריאותי, הנפשי הכלכלי וכד', ואף מעניק הרשאות רחבות בגישה ושימוש במידע על אודותיו, מבלי שיהיה מודע בהכרח לאופן השימוש במידע ולהעברתו לגורמים אחרים. מאפיין נוסף של מגזר זה הוא עצם ניהול והחזקת כמויות גדולות של מידע רפואי רגיש בידי גופים פרטיים.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותם ארגונים לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית, ועמידה בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר.

נוכח אלה הרשות להגנת הפרטיות הגדירה מגזר זה כיעד פיקוח רוחב משמעותי.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל-10 גופים המעניקים שירותי סיוע במימוש זכויות רפואיות, כאשר במסגרת בחירת הגופים נלקחו בחשבון היקפי המידע וכמות הלקוחות, ורגישות המידע במסגרת השירותים הניתנים ללקוחות.

שאלוני הביקורת בחנו חמישה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית וממשל תאגידי, ניהול מאגרי מידע, העברת מידע בין גופים ציבוריים, אבטחת מידע ושימוש בשירותי מיקור חוץ. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם ואשר נבחנו על ידי הרשות, בהתאם לרמת עמידתם בהוראות חוק הגנת הפרטיות והתקנות מכוחו.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר מימוש זכויות רפואיות נמצאה רמת עמידה בינונית בכל הקשור בבקרה ארגונית וממשל תאגידי בתחומי הגנת הפרטיות אשר באה לידי ביטוי בעיקר באי מינויים של מנהלי מאגר מידע ועדכון הרשם בעניין כנדרש, קביעה חלקית של נהלי אבטחת מידע והליך מיון עובדים שאינו בהתאם לדרישות התקנות. נמצאה רמת עמידה בינונית-גבוהה בהוראות חוק הגנת הפרטיות והתקנות מכוחו בכל הקשור בניהול מאגרי מידע, כאשר הליקויים העיקריים נבעו מאי רישום מאגרים אלו בפנקס המאגרים, אי מתן הודעה לנושא המידע בעת איסוף המידע בהתאם לחוק, ושימוש במאגרי המידע למטרות נוספת מעבר למטרה לשמה נאסף.

כמו כן, נמצאה רמת עמידה בינונית-נמוכה בכל הקשור לעיבוד מידע אישי בהסתייעות בשירותי מיקור חוץ ובמיוחד בנוגע לשלבי ההיערכות להתקשרות עם צד ג' למתן שירותי עיבוד מידע אישי בחברה, לאופן עיבוד המידע האישי במיקור חוץ עם ספקי מיקור חוץ בחברה, וכן בנושא נקיטת פעולות בכדי לוודא שצד ג' נוקט באמצעים הנדרשים כדי להגן על מאגרי המידע.

מפיקוח הרוחב עולה גם כי חלק הארגונים אינם מיישמים באופן מלא מדיניות אשר תואמת את דרישות החוק והתקנות בכל הקשור לנושאי אבטחת מידע. נמצאו מקרים בהם לא באו לידי ביטוי האמצעים בהם נוקט הארגון בכל הקשור להרשאות, אמצעי ההגנה, ואופן אמצעי הזיהוי והשימוש בשיטות הצפנה.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 7 גופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם, כאשר שני גופים מפוקחים מכלל הגופים שנבדקו ואשר סיימו את פעילותם, קיבלו הנחיות מתאימות בנוגע לאופן מחיקת רישום מאגרי המידע שברשותם. לאור בחינת הליקויים שאותרו במגזר, דו"ח זה כולל ריכוז של ההנחיות העיקריות לתיקון הליקויים שנשלחו לגופים.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

ממצאי הליך פיקוח רוחב
בקרב מגזר נותני שירותי סיוע במימוש זכויות רפואיות

דו"ח פיקוח רוחב 2019-2020

אתגרים ומאפיינים ייחודיים של מגזר נותני שירותי סיוע במימוש זכויות רפואיות

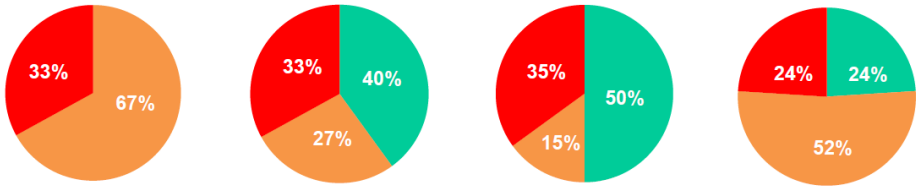
ניהול והחזקת כמויות גדולות של מידע רגיש בידי גופים פרטיים.

יחסים ייחודיים ופערי כוחות מובנים בין נותן השירות ומוסר המידע, אשר מוסר מידע רגיש, לרבות מידע אודות מצבו הבריאותי, הנפשי, הכלכלי וכד'.

מתן הרשאות רחבות בגישה ושימוש במידע על-ידי הלקוח לנותן השירותים, מבלי שיהיה מודע בהכרח לאופן השימוש במידע ולהעברתו לגורמים אחרים.

התהליך שבוצע במספרים

ממצאי נותני שירותי סיוע במימוש זכויות רפואיות



- רמת עמידה גבוהה
- רמת עמידה בינונית/חלקית
- רמת עמידה נמוכה

עיקרי ההנחיות לתיקון ליקויים

ניהול מאגרי מידע

מתן הודעה לנושא המידע 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.

על הגוף להסדיר ולעדכן את רישום המאגרים בפנקס מאגרי המידע. יש לפעול לפי סעיף 8 (ג) לחוק הגנת הפרטיות.

שימוש במידע שבמאגרי המידע בחברה ייעשה רק למטרה שלשמה הוקם מאגר המידע.

בקרה ארגונית וממשל תאגידי

יש לעדכן את הרישום בפנקס המאגרים בדבר זהות מנהל המאגר בהתאם לנדרש בחוק ולהכין כתב מינוי רשמי לכלל מנהלי המאגרים בארגון.

בחינת הצורך בהכנת תכנית לבקרה שוטפת על העמידה בדרישות התקנות בהתאם לתקנה 3 לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017 (תקנות אבטחת מידע). וכתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.

בהתאם לתקנה 7 לתקנות אבטחת מידע, יש לוודא כי במהלך הליכי המיון לעובדים חדשים ושיבוצם נבחן האם אין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר, בדגש על אמינות, שמירת סודיות וכיוצ"ב.

שירות מיקור 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.

על הגופים, בעלי המאגר, לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, כאשר יש לקבוע במפורש בהסכם את חובותיו ואחריותו של הספק, בהתאם להוראות תקנות אבטחת מידע, לרבות דיווח אודות אירועי אבטחת מידע, מנגנוני אבטחת המידע הנדרשים, שמירת המידע לאחר סיום תקופת ההתקשרות וחובות צד ג' בהעברת מידע לאחר.

בחינה וביצוע של כלל הפעולות הנדרשות בהתאם לתקנה 15 ולהנחיית 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.

יש לוודא כי כל גוף צד ג' אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.

אבטחת מידע

יש להטמיע מנגנון הרשאות המבוסס על הצורך לדעת ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עקרון זה.

בהתאם לתקנות אבטחת מידע, תקנה 14 (ב), העברת מידע ממאגרי המידע ברשת ציבורית או האינטרנט תיעשה באמצעות שימוש בשיטות הצפנה מקובלות בלבד (TLS 1.2 ומעלה).

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.

אופן הזיהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.

2. נותני שירותי סיוע במימוש זכויות רפואיות - תמונת מצב

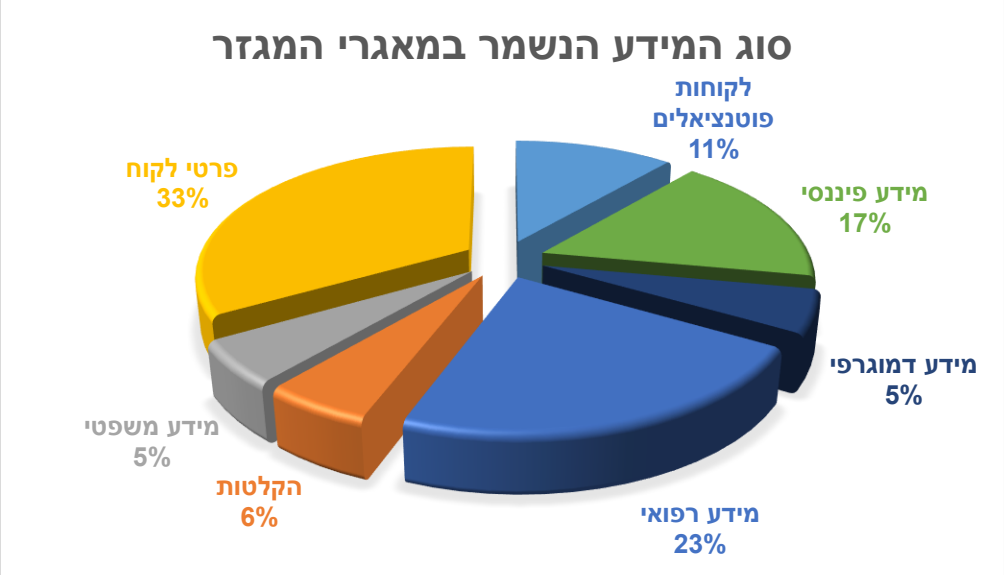
2.1. כללי

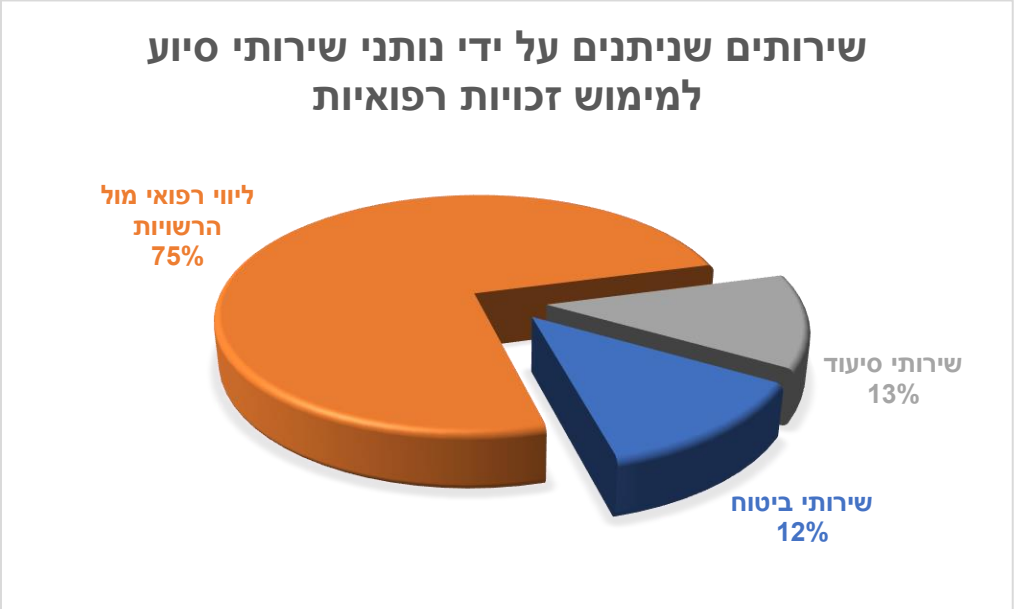
הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למאי 2020 במגזר נותני שירותי סיוע במימוש זכויות רפואיות.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר מימוש זכויות רפואיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים, וזאת בשל מאפייניו הייחודיים של מגזר זה בהיבטי הפרטיות. מאפיינים אלו באים לידי ביטוי ביחסים ייחודיים ופערי כוחות מובנים בין נותן השירות ומוסר המידע, אשר מוסר מידע רגיש לרבות בנוגע למצבו הבריאותי, הנפשי הכלכלי וכדומה, ואף מעניק הרשאות רחבות בגישה ושימוש במידע על אודותיו, מבלי שיהיה מודע בהכרח לאופן השימוש במידע ולהעברתו לגורמים אחרים. מאפיין נוסף של מגזר זה הוא עצם ניהול והחזקת כמויות גדולות של מידע רפואי רגיש בידי גופים פרטיים.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב אותם ארגונים לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית ועמידה בהוראות החוק בכל הנוגע לדיווח ישיר ולשירותי דיווח ישיר.





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, ולתכנית העבודה השנתית של הרשות. התכנית נבנית בהתחשב בקריטריונים הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות, והצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

הליך הפיקוח בוצע ב- 10 גופים, במגזר מימוש זכויות רפואיות, שנבחרו על ידי הרשות תוך בחינת היקפי המידע וכמות הלקוחות, ורגישות המידע במסגרת השירותים הניתנים ללקוחות., בניכוי גופים אשר סיימו פעילותם, שינו פעילות, דיווחו על פעילות שאינה רלוונטית למגזר הנבדק. לאחר איחוד גופים אשר השיבו מענה מאוחד בשל פעילות עסקית מאוחדת או ניהול שימוש במאגר או תשתית טכנולוגית משותפת, נמצאו תחת פיקוח 7 גופים. במסגרת התהליך שני גופים אשר דיווחו על סיום פעילותם נדרשו למחוק את רישום מאגר המידע שבידם, שני גופים נדרשו לספק מידע, מסמכים והבהרות נוספות לרשות, כאשר עבור אחד מאותם הגופים נקבע להשלים ולאמת ידיעות ומסמכים באמצעות פיקוח במשרדי הגוף המפוקח, אשר לא בוצע בסופו של יום עקב משבר הקורונה, והושלמו באמצעות דרישות השלמות מידע בכתב. בסיום ההליך, נמצאו בכל אחד מ-7 הגופים המפוקחים ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את אותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, עשויה הרשות לבדוק באמצעות ביקורת חוזרת את השלמת התיקונים אצל כלל המפוקחים או חלקם, בהתאם לשיקול דעתה.

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

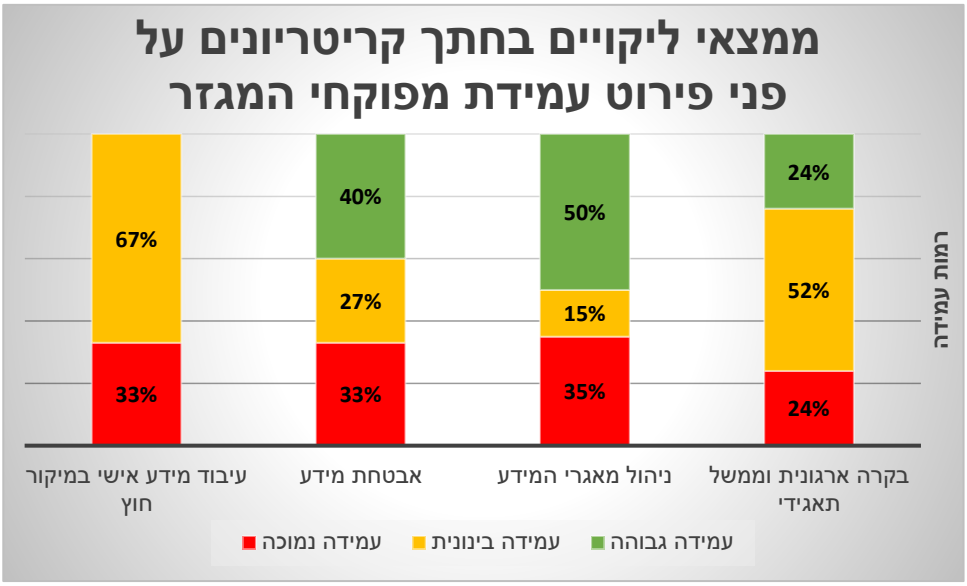
במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לקריטריונים שונים ובהם:

- **בקרה ארגונית וממשל תאגידי** - קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע 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, ועמידה 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 צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע.
- **העברת מידע אישי בין גופים ציבוריים** - בחינת קיומן של ועדות הבוחנות את הצורך במידע במרפאות המשתייכות לגופים ציבוריים, אי-העברת מידע עודף, והסמכות להעברה וקבלת מידע מגופים ציבוריים ואליהם.

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 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.

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

- במסגרת בחינת קריטריון זה, נמצא כי 76% מהגופים עמדו ברמה בינונית-נמוכה בהוראות החוק בנוגע לבקרה ארגונית וממשל תאגידי.
- במסגרת השאלות בקריטריון הממשל התאגידי, השיבו חלק מהגופים כי לא מינו מנהלי מאגרים. גם כאשר מונו כאלו, הדבר לא דווח כנדרש לרשם המאגרים.
- נמצאו גופים אשר אין להם תיעוד מסודר לנהלי אבטחת מידע או שהנהלים שהתקבלו אינם מספיק איכותיים בכך שאינם מקיפים את כלל הדרישות בהוראות התקנות.
- כמו כן, נמצאו פערים בנושא ביצוע בדיקת התאמה לעובדים חדשים בעלי גישה למאגר, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר.

3.2. ניהול מאגרי מידע

- במסגרת בחינת קריטריון זה, נמצא כי 50% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לניהול מאגרי מידע, אולם ב-50% מהגופים הנותרים נמצאה רמת עמידה בינונית נמוכה, הבאה לידי ביטוי בליקויים באופן יישום הוראות החוק והתקנות.
- מקרב הגופים שנמצאה בהם רמת עמידה בינונית-נמוכה, נמצאו גופים רבים אשר לא עמדו בדרישות החוק בנוגע לרישום מאגרי המידע.

- נמצאו ליקויים ביישום הוראות החוק בכל הנוגע לשקיפות בדבר מקור הסמכות לאיסוף המידע האישי מול נושאי המידע והיידוע בדבר זכויותיהם בנוגע למאגר המידע הרפואי בו נשמרים פרטיהם.

3.3. אבטחת המידע

- בקריטריון זה נמצאה רמת עמידה גבוהה ב- 40% בלבד מהגופים, בעוד שב- 60% מהגופים, נמצאו רמות עמידה בינונית ונמוכה.
- בין היתר, נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בהעדר תהליכים נאותים לניהול הרשאות ובין אם בהעדר יישום הפרדת תפקידים ויישום מתן הרשאה לפי עקרון הצורך לדעת בלבד (בעל ההרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות).
- אותרו גופים אשר לא נקטו באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את מאגרי המידע או המאפשרים גישה אליהם.
- בנוסף, נמצאו גופים אשר בכניסה למאגר המידע באמצעות רשת האינטרנט, לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- כמו כן, נמצאו ליקויים רבים בנושא אבטחת אמצעים נתיקים, בין אם בהעדר הגבלות על שימוש באמצעים אלו או בהעדר הצפנה נאותה.

3.4. עיבוד מידע אישי במיקור חוץ

- **הליקוי המרכזי שנמצא במגזר זה** מתייחס לקריטריון עיבוד מידע אישי במיקור חוץ בו 33% מהגופים נמצאו ברמת עמידה נמוכה, 77% ברמת עמידה בינונית, כאשר אף גוף לא עמד בקריטריון זה ברמת עמידה גבוהה.
- מהממצאים עולה כי מרבית הגופים אינם מבצעים התקשרות עם ספקי מיקור חוץ בהתאם לדרישות הקבועות בתקנות, לא בוחנים את איכות ניהול אבטחת המידע ואת אופן תפעול מאגרי המידע אצל ספקי מיקור החוץ ולא מבצעים פעולות פיקוח כנדרש.
- 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, הנובעת משימוש במיקור חוץ.

4. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר מימוש זכויות רפואיות 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**:

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, תוך התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.

על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע היכן שנדרש למנות כזה, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לתקנה 3 לתקנות 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'. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות אבטחת מידע (תקנה 4).

כמו כן, על הגופים להכין תכנית עבודה לנושא אבטחת מידע והגנת הפרטיות לרבות התייחסות לנושא גורם אחראי ולו"ז לביצוע, שתעמוד בדרישות תקנות אבטחת מידע (תקנה 3 (3)). ככל שמדובר בגוף החייב במבדקי חדירות, עליו לוודא כי אכן נעשו כאלה העומדים בדרישות תקנות אבטחת מידע (תקנה 16).

בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או כל גורם אחר שמקבל גישה למאגר/מערכת הכוללת מספר מאגרים.

4.2. ניהול מאגרי מידע

מכוח החובה המוטלת על פי החוק, על הגופים המנהלים רשימות מטופלים הכוללות אפיון של נושאי המידע לרבות מידע עליהם, כהגדרתו בחוק הגנת הפרטיות, 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.

בנוסף, 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 המצולמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי על ידי בתי עסק או גוף אחר הנותן שירות לציבור. כמו כן, יש להקפיד לאפשר לנושאי המידע לתקן או 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 ו-9 (א) לתקנות אבטחת מידע, אשר יבטיחו הפרדת סמכויות ויאפשרו גישה לנתוני המאגר אך ורק במידה הנדרשת לביצוע התפקיד של העובדים בעלי הגישה למידע.

בנוסף, על הגופים לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע. כמו כן, עליהם לוודא שבכניסה לאתר מאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה על פי תקנות אבטחת מידע (תקנה 9(ב)(2)).

במאגרים בעלי רמת אבטחה גבוהה, יש לבצע מבדקי חדירה אחת ל-18 חודשים, בהתאם לתקנה 5(ד) לתקנות אבטחת מידע.

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.

4.4. 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 בעלי המאגר לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הוראות תקנה 15(א)(2) לתקנות 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 המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי" .

5. סיכום

כאמור, מגזר מימוש זכויות רפואיות מעלה סיכונים לא מעטים לפרטיות לקוחותיו, אשר נובעים מניהול מידע רב, מזוהה ורגיש, וניהול קשר ישיר עם ציבור הלקוחות באמצעות הגופים ובאמצעות גופי מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות אבטחת מידע, שקיפות מול הלקוח, ומילוי החובות החלות מכוח פרק הדיוור הישיר בחוק הגנת הפרטיות.

ממצאי הליך פיקוח הרוחב במגזר מימוש זכויות רפואיות העלה ממצאים מדאיגים המצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ, עמידה חלקית בהוראות החוק בכל הנוגע למינוי ממונה אבטחת מידע ופערים ברמת האבטחה הקיימת ביחס לניהול הרשאות גישה למאגרי המידע. בנוסף, נמצא כי חלק מהגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את ציבור המטופלים בדבר זכויותיהם על פי חוק הגנת הפרטיות בקשר לפניות המועברות אליהם בדיוור ישיר, הכוללות בין היתר את החובה להציג את מקור המידע.

ניכר, כי עצם קיום הליך פיקוח הרוחב 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 התחייבות נושא משרה ותכנית מסודרת לתיקון הליקויים.

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 במגזר מימוש זכויות רפואיות, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית וממשל תאגידי			
לא צוין הגורם שביצע את ביקורת אבטחת המידע.	על הארגון לוודא כי ביקורות בנושא אבטחת מידע מבוצעות על ידי גורם בלתי תלוי.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, תקנה 16	**ביקורות תקופתיות**
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**
לא ניתן מענה בשאלון להליך מתן גישה למאגר לכן לא ניתן לבחון האם ההליך תואם לתקנות.	יש לבחון האם הליך מתן גישה למאגר תואם לכללים שנקבעו בתקנות.	אבטחת מידע בניהול כוח אדם –קליטת עובדים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 7	**מיון עובדים חדשים**
בכתב המינוי של ממונה אבטחת מידע לא פורטו תחומי האחריות ולכן לא ברור האם הינו ממלא תפקיד נוסף שיכול להוות חשש לניגוד עניינים	יש לוודא כי ממונה אבטחת המידע אינו משמש בתפקיד נוסף שיכול להעמיד אותו בניגוד עניינים.	חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3	**מינוי ממונה אבטחת מידע**
ממונה על אבטחת מידע בארגון ממלא תפקיד נוסף העשוי להעמידו בחשש לניגוד עניינים.	יש למנות כממונה אבטחת מידע אדם בעל הידע המתאים, שאינו מצוי בניגוד 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 הועבר תיעוד של נוהל אבטחת מידע	יש לבחון האם נוהל אבטחת המידע עומד בהוראות תקנות הגנת הפרטיות.	נוהל אבטחת מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4	**נהלי אבטחת מידע**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
נוהל אבטחת מידע אינו מעודכן.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם.	נוהל אבטחת מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4 (ה)	**נהלי אבטחת מידע**
נוהל אבטחת המידע אינו כולל התייחסות לצורך בעדכון שנתי.	יש לעגן בנוהל העבודה בנושא אבטחת המידע את נושא תדירות עדכון הנהלים.	נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נהלי אבטחת מידע**
לא הועבר תיעוד של תכנית העבודה.	יש לבחון האם תכנית העבודה השנתית מכסה בצורה טובה את נושאי אבטחת מידע והגנה על הפרטיות והאם היא מפרטת את הגורם האחראי ואבני דרך ברורים.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
תכנית העבודה השנתית לאבטחת מידע והגנת הפרטיות אינה כוללת הגדרת גורם אחראי.	יש להקפיד כי תכנית לטיפול בליקויים תכלול התייחסות והגדרת הגורם האחראי לטיפול.	תכנית עבודה שנתית לבקרה שוטפת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
לא הועבר תיעוד של תכנית עבודה שנתית.	יש למסור מסמכים מבססים.	תכנית עבודה שנתית לבקרה שוטפת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
ניהול מאגרי מידע			
לא נמסרת הודעה לנושא המידע בעת קבלת מידע אודותיו	מתן הודעה לנושא המידע 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.	חובת מבקש המידע חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11	**מקור סמכות לאיסוף המידע**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא מתאפשר לנושא המידע לתקן או לשנות את המידע אודותיו במאגרי המידע.	רצוי לאפשר לנושא המידע לבקש לתקן את המידע שעליו המוחזק במאגר המידע, במידה ומצא כי המידע עליו אינו נכון/ שלם/ ברור או מעודכן.	חוק הגנת הפרטיות, תשמ"א-1981,סעיף 14	**מקור סמכות לאיסוף המידע**
לא קיים רישום מאגרים של לקוחות, לקוחות פוטנציאליים ועובדים אצל רשם מאגרי המידע.	יש לפעול להסדרת רישום מאגרי המידע בהקדם.	חוק הגנת הפרטיות תשמ"א – 1981, סעיף 8	**רישום המאגר אצל רשם**
אבטחת מידע			
לא קיימים אמצעי אבטחה מספקים, או פירוט מעמיק במיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את או המאפשרים גישה אל מאגרי המידע בכדי למנוע חדירה וכניסה ללא הרשאה בהתאם לדרישה בתקנות.	במאגרי מידע בהם חלה רמת אבטחה בינונית ומעלה, נקיטת אמצעי אבטחה למיקום הפיזי בו נשמרות מערכות המאגר, בכדי למנוע חדירה וכניסה ללא הרשאה, הכוללים אמצעים לבקרה ולתיעוד של הכניסה והיציאה מהאתרים שבהם מצויות המערכות.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017,תקנה 6	**אבטחה פיזית**
אין אמצעי הגנה למאגרים המחוברים לאינטרנט.	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**
התחברות מרחוק אינה מבוצעת באמצעות FA2.	יש להטמיע מנגנון דו שלבי בהתחברות מרחוק (לדוגמה: טוקן, OTP).	אבטחת תקשורת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (ג). תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב)(2).	**גישה מרחוק**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא קיימת הפרדה בין המאגרים המכילים מידע אישי לבין יתר תשתיות הארגון.	הפרדה בין מערכות המאגר אשר ניתן לגשת מהן 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)	**הפרדה בין מאגרים**
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.	אפיון ויישום תהליך בו מיד בעת סיום תפקיד או עזיבת עובד הארגון, הרשאותיו של העובד יבוטלו או יעודכנו בהתאם לצורך.	זיהוי ואימות בעת התחברות למאגר מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ג)	**ניהול הרשאות**
בגוף המפוקח קיימים מאגרים בעלי רמת אבטחה גבוה בהם לא בוצעו מבחני חדירה.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה מידי אחת לשנה וחצי, בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 5(ד).	**מבדקי חדירה**
לא ניתן מענה למדיניות הסיסמאות הקיימת במאגרים בהם מנוהל מידע רפואי אישי.	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'	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב-2)	**מדיניות סיסמאות**
לא ניתנה תשובה מפורטת בקשר למנגנון ההרשאות (לא צוין האם ההרשאות הן בהתאם לצורך לדעת, כיצד מעודכנות הרשאות בעת שינוי תפקיד וכו').	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.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017 תקנה 9	**ניהול הרשאות**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
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 נערך בארגון סקר סיכוני מערכות מידע.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים מידי אחת לשנה וחצי, בחינה את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.	סקר סיכונים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 5(ג)	**סקר סיכונים**
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**
לא ניתן פירוט אודות אופן הטיפול באירועי אבטחת מידע והמנגנונים הקיימים לצורך איתור אירוע כאמור.	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**
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.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ	**מיקור חוץ**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
	3. שמירת המידע לאחר סיום תקופת ההתקשרות. 4. חובות צד ג' בהעברת מידע לאחר.	(Outsourcing) לעיבוד מידע אישי.	
לא קיים הסכם מול ספק מיקור החוץ.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 והנחיות רשם מאגרי המידע מס' 2/2011 עבור כל 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-2017, תקנה 15. הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**