משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

דו"ח פיקוח רוחב

2018-2019

ממצאי הליך פיקוח הרוחב בקרב מגזר מועדוני הלקוחות בישראל



כסלו תש"פ
דצמבר 2019

תוכן עניינים

1. תקציר מנהלים 3
1.1. פיקוחים מגזריים 3
1.2. מגזר מועדוני לקוחות 3
1.3. תהליך העבודה 4
1.4. ליקויים, מסקנות והמלצות עיקריות 4
2. מועדוני לקוחות - תמונת מצב 5
2.1. כללי 6
2.2. רקע על המגזר 6
2.3. תהליך העבודה 7
2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות החוק 7
3. ממצאים – ליקויים מרכזיים 8
3.1. בקרה ארגונית וממשל תאגידי 9
3.2. ניהול מאגרי מידע 9
3.3. אבטחת המידע 9
3.4. עיבוד מידע אישי במיקור חוץ 10
4. מסקנות/תמונת מצב והמלצות 10
4.1. בקרה ארגונית וממשל תאגידי 10
4.2. ניהול מאגרי מידע 10
4.3. אבטחת מידע 11
4.4. עיבוד מידע אישי במיקור חוץ 12
5. סיכום 13

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם 14

1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות, אשר נוסף בשנת 2018 לזרועות האכיפה המנהלית והפלילית ברשות, 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 הגנת הפרטיות "אבטחת מידע"), במטרה לאתר הפרות של החוק, להגברת מודעות המשק להוראות החוק, להגברת האכיפה היוזמת של הרשות, לאיתור כשלים ענפיים הדורשים התייחסות והנחיות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות החוק.

הרשות להגנת הפרטיות מפרסמת את ממצאי פעילות מערך פיקוחי הרוחב אותה ביצעה בקרב עשרות גופים במגזרים שונים, אשר מנהלים או מחזיקים במאגרי מידע בעלי רגישות מיוחדת, בין היתר, בשל רגישות והיקפי המידע, האתגרים הטכנולוגיים, מידע אודות קטינים ועוד. מאגרים אלה נדרשים לעמידה קפדנית בהוראות החוק והתקנות על מנת למנוע שימוש לרעה במידע האישי וכן על מנת למנוע אפשרות של אירועי אבטחה חמורים.

1.1. פיקוחים מגזריים

במסגרת הליך פיקוח הרוחב לשנים 2018-19, 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 ספקי פלטפורמות אינטרנטיות לימודיות אשר אוספות מידע על קטינים ו- 36 חברות המספקות שירותי אחסון ועיבוד מאגרי מידע. בנוסף, הרשות ערכה 54 פיקוחי רוחב יעודיים 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 מועדוני הלקוחות, על אתגריו המיוחדים ומסקנותיו המגזריות. דוחות מסכמים נוספים על המגזרים הנ"ל מפורסמים באתר הרשות.

1.2. מגזר מועדוני לקוחות

בשנת 2018 הרשות להגנת הפרטיות הגדירה את מגזר מועדוני הלקוחות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה, המנהל או מחזיק מאגרי מידע רבים המתייחסים למידע רגיש ומזוהה אודות הרגלי צריכה, ומנהל קשר אינטראקטיבי עם ציבור לקוחותיו, בין אם באופן ישיר ובין אם באמצעות שירותי מיקור חוץ. ניהול הקשר עם הלקוחות מחייב את אותם ארגונים בלעמוד בדרישות אבטחת המידע, לקיים את חובת השקיפות אל מול הלקוח (כמו לדוגמה למסור ללקוח כי הוא אינו חייב למסור את המידע אם אין חובה חוקית לכך), ולעמוד בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר.

1.3. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב הרשות פנתה בדרישה למילוי שאלוני ביקורת ל-54 גופים המנהלים מועדוני לקוחות. מועדונים אלה מחזיקים, כל אחד, במידע אודות למעלה ממאה אלף לקוחות[1].

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 מועדוני הלקוחות נמצאה רמת עמידה נמוכה בהוראות חוק הגנת הפרטיות בנוגע להסתייעות בשירותי מיקור חוץ לשם ביצוע פעולות לעיבוד מידע אישי הכולל בין היתר פרטי קשר, מידע דמוגרפי, קשרים משפחתיים, מידע אודות הרגלי צריכה או התנהגות, השתייכות דתית וכד'. כמו כן, עולה כי במרבית החברות במגזר מועדוני הלקוחות לא פועלים על פי הוראות החוק בכל הנוגע למינויים של מנהלי מאגרים. כמו כן, מרבית מהגופים המשתייכים למגזר זה נמצאו ככאלה שאינם מקפידים ליידע את ציבור הלקוחות על האופן שבו נאסף המידע אודותיהם, אינם מיידעים את הלקוחות בדבר זכויותיהם מכוח חוק הגנת הפרטיות, כמו למשל, החובה להציג את מקור המידע, הזכות לעיין במידע והזכות להימחק ממאגר המידע.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 43 גופים מתוך 44 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם. לאור בחינת כשלי המגזר, כולל דו"ח זה הנחיות לכלל הגופים הפועלים במגזר זה, באשר לצעדים שעליהם לנקוט בכדי לעמוד בדרישות החוק והתקנות.

[1] מדובר בגופים אשר דיווחו לרשות להגנת הפרטיות כי מנהלים מועדון לקוחות ומחזיקים בלמעלה ממאה אלף רשומות אודות נושאי מידע.

דו"ח פיקוח רוחב 2018-2019

ממצאי הליך פיקוח הרוחב בקרב מגזר מועדוני הלקוחות בישראל

כסלו תש"פ, ינואר 2020

אתגרים ומאפיינים ייחודיים של מגזר מועדוני לקוחות

- רמת השקיפות הנדרשת בתהליך הרישום למועדון הלקוחות
- ניהול והחזקת כמויות גדולות של מידע אישי רגיש
- חובות החלות מכח דיווח ישיר

התהליך שבוצע במספרים

- **54** שאלונים שהופצו
- **7** גופים נדרשו לבער את המאגר
- **16** דרישות להשלמת מידע חסר בכתב ובפיקוח בשטח
- **43** הנחיות לתיקון ליקויים

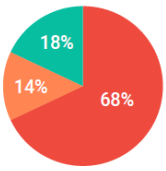
התנעה

ממצאים- ליקויים מרכזיים

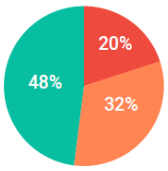
רמת עמידה גבוהה
עמידה של בין 100%-80% בקריטריונים

רמת עמידה בינונית/חלקית
עמידה של בין 80%-50% בקריטריונים

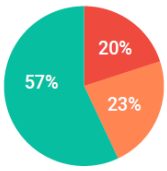
רמת עמידה נמוכה
עמידה של מתחת ל-50% בקריטריונים



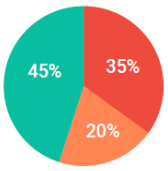
עיבוד מידע אישי במיקור חוץ



אבטחת מידע



ניהול מאגרי המידע



בקרה ארגונית וממשל תאגידי

עיקר ההנחיות לתיקון ליקויים



- עדכון ניהול מועדון הלקוחות כאחת ממטרותיו ומאפייניו של מאגר המידע
- בדיווח ישיר יש להקפיד על ציון הפרטים המנויים בסעיף 17' לחוק
- יידוע ומתן אפשרות לנושאי המידע לעיין במידע על אודותם, המוחזק במאגר מידע בהתאם לחוק
- רישום המאגרים לגביהם קיימת חובה לרשמם בפנקס מאגרי המידע
- בחינת החובה למנות ממונה אבטחת מידע
- עריכת הסכם שמטרתו להבטיח הגנה על המידע האישי המועבר לצד שלישי הנותן שירותי עיבוד ואיחסון
- נקיטת אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות תקנות אבטחת מידע ובהוראות ההסכם שנחתם עמו המתייחס לחובותיו להגן על המידע
- הקפדה על ביצוע הדרכה והכשרה לבעלי הרשאות
- קביעת נוהל אבטחת מידע ועדכונו בהתאם לתקנה 4 לתקנות אבטחת מידע
- הגבלת החיבור ושימוש באמצעים נתיקים לצרכים הכרחיים בלבד
- וידוא בניית מנגנוני הרשאות במאגרי המידע של הארגון בהתאם לתקנה 8 ותקנה 9 (א) לתקנות אבטחת המידע

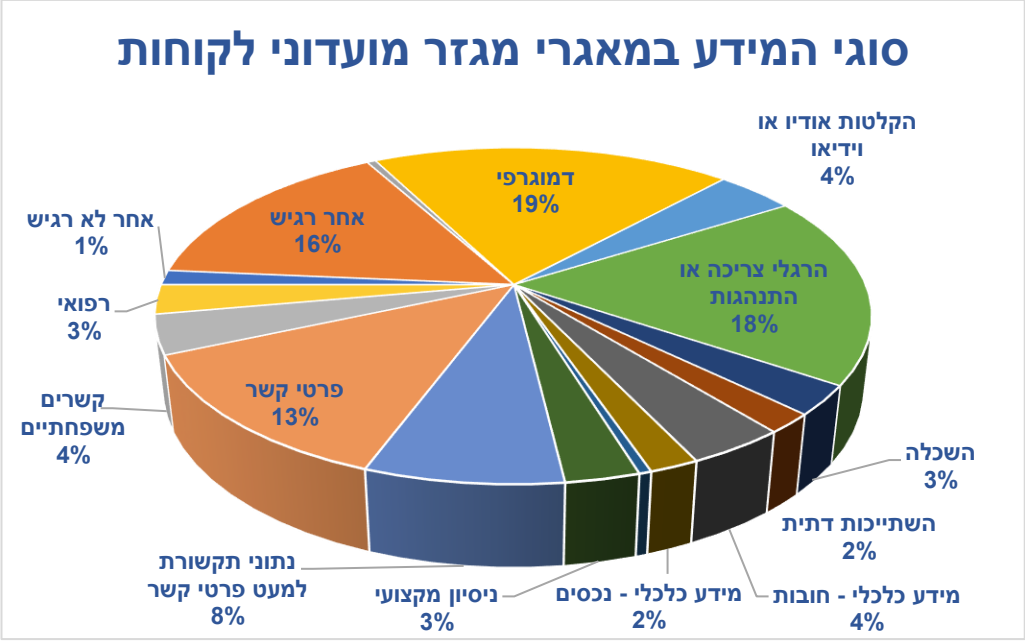
2. מועדוני לקוחות - תמונת מצב

2.1. כללי

הדו"ח המונח לפניכם, הינו הדו"ח המתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2018 לאוגוסט 2019 במגזר מועדוני הלקוחות.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר מועדוני הלקוחות כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר. ראשית, חברות המנהלות מועדוני לקוחות, מחזיקות במידע רב על אודות מספר רב של אנשים או לקוחות. שנית, אותן חברות מנהלות עם נושאי המידע קשר אינטראקטיבי המאפשר לאותן חברות לזהות וללמוד לא רק את הרגלי הצריכה של נושאי המידע, אלא גם מאפיינים ייחודיים לגבי אישיותם, מצבם הכלכלי, השתייכותם הדמוגרפית, אמונתם וכד'. היקפי המידע ומספרם הרב של האנשים עליהם מוחזק המידע דורשים הקפדה מיוחדת על אבטחת המידע, קיום חובת השקיפות כפי שפורטה לעיל, ועמידה בהוראות החוק לעניין דיוור ישיר ושירותי דיוור 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, 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 מועדוני הלקוחות, בחרה הרשות גופים המנהלים מאגרי מידע הרשומים בפנקס מאגרי המידע, וביתר פירוט: גופים שאחת ממטרות המאגר הרשומות שלהם הינה ניהול מועדון לקוחות, בהיקפים של למעלה ממאה אלף איש. בחירה זו אפשרה לרשות לפנות לגופים הרלוונטיים ביותר, בעלי סיכונים הנובעים מהיקפי המידע הגדולים שהם מחזיקים ורגישות המידע.

השאלונים נשלחו ל- 54 גופים המנהלים מועדוני לקוחות, כאשר בניכוי גופים אשר סיימו פעילותם, שינו פעילות, דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, ולאחר איחוד גופים אשר השיבו מענה מאוחד בשל פעילות עסקית מאוחדת או ניהול שימוש במאגר או תשתית טכנולוגית משותפת, נמצאו תחת פיקוח 44 גופים. במסגרת התהליך 7 גופים אשר דיווחו על סיום פעילותם נדרשו לבער את מאגר המידע שבידם, 16 גופים נדרשו לספק מידע, מסמכים והבהרות נוספות לרשות, כאשר באחד מאותם הגופים הושלמו ואומתו ידיעות ומסמכים באמצעות פיקוח במשרדי הגוף המפוקח. בסיום ההליך מתוך 44 הגופים המפוקחים, נמצאו ב-43 מתוכם ליקויים הדורשים תיקון. בהתאם לכך, הפיצה הרשות לאותם גופים מכתבים בהם נדרשו הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים, כאשר כחלק מההליך תבדוק הרשות באמצעות ביקורת חוזרת את השלמת התיקונים בגופים נבחרים.

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:

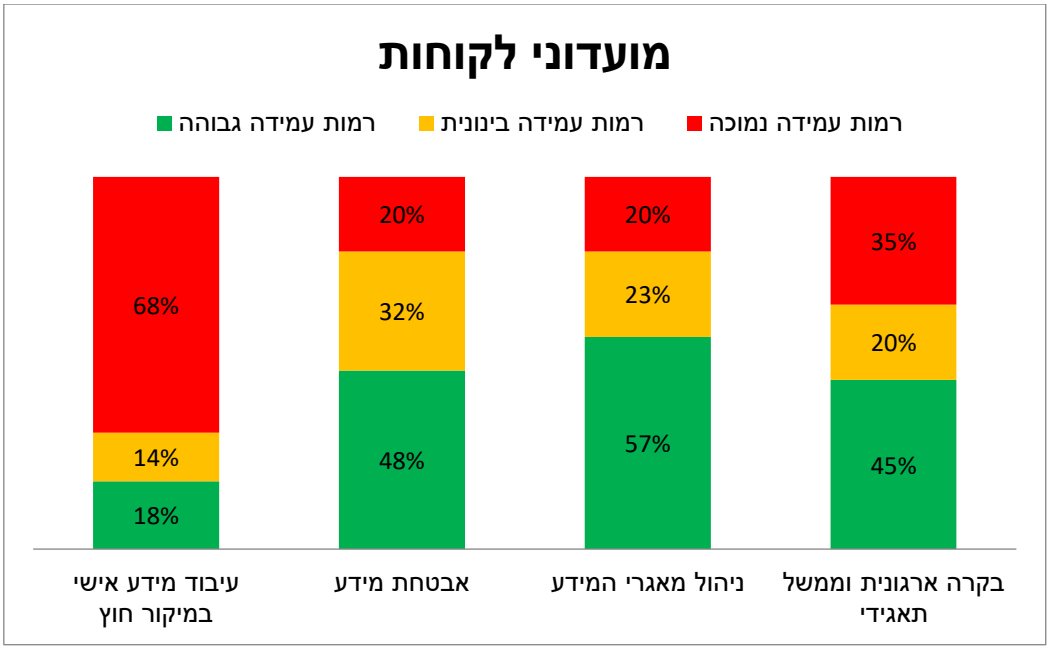
- **בקרה ארגונית וממשל תאגידי** - קריטריון זה בוחן קיומה של תכנית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** – קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק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

- **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 (65%) נמצאה רמת עמידה בינונית עד נמוכה בהוראות החוק בנוגע לבקרה הארגונית וממשל תאגידי.
- כחלק מאי העמידה בדרישות הממשל התאגידי, נמצאו ליקויים בהגדרת מאגר המידע ומטרותיו ואי מילוי הדרישה למינוי של מנהלי מאגרים. גם כאשר מונו כאלו, נמצאו גופים מפוקחים אשר מינו בעלי תפקידים ללא כתב מינוי או עם כתב מינוי אשר אינו כולל את מהות התפקיד.
- נמצאו ארגונים ללא מסמך הגדרות המאגר אותו הם מנהלים.
- נמצאו גופים בהם תפקידים ותחומי אחריות היו מרוכזים אצל גורם יחיד באופן אשר עלול להוות ניגוד עניינים, בניגוד לדרישות תקנות הגנת הפרטיות (אבטחת מידע).
- ליקוי נוסף נמצא בגופים אשר מהווים נציגות או סניפים של גופים בינלאומיים המנהלים מועדוני לקוחות, אשר הסתמכו על נהלי הישות הבינלאומית בכל הנוגע לסוגיות הפרטיות ואבטחת המידע, בעוד שבפועל לא הוטמעה וללא שנעשה תהליך שמטרתו לוודא כי פעילות הארגון עומדת בקנה אחד עם הדין הישראלי בתחום הפרטיות.
- כמו כן, במרבית מהגופים שנבחנו, נמצא כי סט הנהלים וההדרכות אשר אמור היה להתייחס לנושא הגנת הפרטיות, כלל התייחסות להיבטי אבטחת מידע בלבד.

3.2. ניהול מאגרי מידע

- במסגרת בחינת קריטריון זה, נמצאו ליקויים משמעותיים בכ43% מהגופים (20% עמידה ברמה נמוכה, ו23% ברמה בינונית). בדגש על ליקויים ביישום הוראות החוק בכל הנוגע להגדרת מאגר המידע ומטרותיו.
- כמו כן, נמצאו ליקויים ביישום הוראות החוק בכל הנוגע לשקיפות בדבר מקור הסמכות לאיסוף המידע האישי ויידוע האנשים עליהם מוחזק המידע, בדבר זכויותיהם ומאגר המידע בו רשומים בעת פנייה בדיוור ישיר.
- מכלל גופים אלו, מרביתם לא הבהירו לנושאי המידע את זכותם לעיין במאגרי המידע ולא ציינו זאת בתקנון שלהם או במסגרת אחרת.

3.3. אבטחת המידע

- במרבית הגופים (52%) נמצאו ליקויים באופן יישום הוראות תקנות הגנת הפרטיות (אבטחת מידע), ביניהם נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בהעדר תהליכים נאותים לניהול ההרשאות ובין אם בהעדר יישום הפרדת תפקידים ויישום מתן ההרשאה לפי עקרון הצורך לדעת בלבד (בעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות).

- בנוסף, נמצאו ליקויים רבים בנושא אבטחת אמצעים נתיקים בין אם בהעדר הגבלות על שימוש באמצעים אלו או בהעדר הצפנה נאותה. כמו כן, גופים בעלי תקן ISO27001 סברו בטעות שהינם פטורים מיישום התקנות והליכי הפיקוח.

3.4. עיבוד מידע אישי במיקור חוץ

- הליקוי המרכזי שנמצא במגזר זה מתייחס לקריטריון עיבוד מידע אישי במיקור חוץ (68% מהגופים נמצאו ברמת עמידה נמוכה, ו14% ברמת עמידה בינונית), ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בארגון, קיים עדיין ליקוי בישום 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.
- מרבית (68%) מהגופים אינם מבצעים התקשרות לפי הוראות התקנות בצורה מספקת, לא בוחנים את איכות ניהול אבטחת המידע ואופן תפעול מאגרי המידע אצל ספקי מיקור החוץ ולא מבצעים פעולות פיקוח כנדרש.

4. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר מועדוני הלקוחות 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, על הגופים לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, וכן לוודא כי קיימת 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 הוצאת כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע היכן שנדרש כזה וכן שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע).

4.2. ניהול מאגרי מידע

החובה המוטלת מכוח החוק על הגופים המנהלים רשימת לקוחות המאפיינות את נושאי המידע באופן הכולל מידע כהגדרתו בחוק, כולל 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. בכלל זה, עליהם לוודא שהגדרת המאגר כוללת מטרה של ניהול מועדון לקוחות[2] וכי הקשר עם הלקוח מוגדר למטרת דיוור ישיר או שירותי דיוור ישיר בהתאם לאופי ההתקשרות שנערכה עם הלקוח.

לעניין התקשורת עם לקוחות, יודגש כי פנייה לנושאי המידע בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או באמצעי אחר, המבוססת על השתייכותם לקבוצת אוכלוסייה מאופיינת, מהווה פנייה בדיוור ישיר כהגדרתה בסעיף 17ג' לחוק. לפיכך, על הגופים להקפיד על ציון הפרטים המנויים בסעיף 17ו' לחוק - לרבות ציון כי הפניה היא בדיוור ישיר, זהותו ומענו של בעל מאגר המידע, מקור המידע, הגורמים להם נמסר המידע, זכותו של מקבל הפניה להימחק מן המאגר המיועד לדיוור ישיר וכד'.[3]

בנוסף, על הגופים להקפיד ליידע ולאפשר לנושאי המידע לעיין במידע על אודותם, 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.[4]

4.3. אבטחת מידע

בהתאם להוראות תקנות הגנת הפרטיות (אבטחת מידע) ובשים לב לליקויים בנושא ניהול הרשאות במאגרי המידע של גופים במגזר זה, על הגופים לוודא שקיימים במאגרי המידע של הארגון מנגנוני הרשאות בהתאם לתקנה 8 ותקנה 9 (א) לתקנות הגנת הפרטיות (אבטחת מידע), שיבטיחו הפרדת סמכויות ויאפשרו גישה לנתוני המאגר רק במידה הנדרשת לביצוע התפקיד של העובדים בעלי הגישה למידע.

כמו כן, נוכח הליקויים שנמצאו בנוגע לשימוש באמצעים נתיקים במגזר זה, על הגורמים הרלוונטיים בגופים לקיים דיון אודות הצורך בחיבור אמצעים נתיקים למערכות הארגון, וככל שיוחלט כי לא קיים צורך ממשי או קיים צורך מינימאלי – עליהם להגביל השימוש למתכונת ההולמת את האלמנטים הבאים: רמת אבטחת המידע שחלה על המאגר, רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד וקיומם 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 המחזיקים בתקן ISO 27001 לפעול בהתאם להנחיית רשם מאגרי המידע 3/2018 – 'תחולת תקנות הגנת הפרטיות (אבטחת מידע) על ארגונים המוסמכים לתקן

---

[2] לקריאה נוספת על רישום מאגר מידע ומטרותיו ר' -
https://www.gov.il/he/Departments/Guides/registration_faq
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

[4] 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

ISO/IEC 27001', בכל הנוגע לקיום דרישות תקנות הגנת הפרטיות (אבטחת מידע) בנוסף לעמידה מלאה בתקן.[5] הרשות רואה ארגון כמי שמקיים את הוראות התקנות במלואן ביחס למאגרים עליהם ניתנה הסמכה לתקן בהתקיים שני תנאים מצטברים: עמידה בתקנות המפורטות בהנחיה והסמכה תקפה לתקן וקיום הוראותיו לרבות כל הבקרות המפורטות בנספח A לתקן, באופן בו הן מפורשות בתקן.

בנוסף, על הגופים לוודא כי קיימים אצלם נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע), וכי נעשית בחינה של תוקפם מעת לעת כנדרש בתקנות.

על הגופים לקבוע הדרכות בנושא אבטחת מידע והגנת הפרטיות לכל עובד חדש בחברה והדרכות ריענון לפחות פעם בשנה לעובדים בעלי גישה למאגרי המידע, ולנהל תיעוד ומעקב אחר הדרכות אלו בהתאם לתקנה 7 לתקנות הגנת הפרטיות (אבטחת מידע.)[6]

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.[7]

---

[5] לקריאה נוספת ר' הנחיית רשם מאגרי המידע 3/2018 - תחולת תקנות הגנת הפרטיות (אבטחת מידע) על ארגונים המוסמכים לתקן ISO/IEC 27001, בכל הנוגע לקיום דרישות תקנות הגנת הפרטיות (אבטחת מידע) בנוסף לעמידה מלאה בתקן -
https://www.gov.il/BlobFolder/policy/iso_iec_27001/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%9E%D7%A1%2003-2018.pdf

[6] 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%9A%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

[7] 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%D

5. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות לקוחות בקרב מגזר מועדוני הלקוחות אשר נובעים מניהול מידע רב, מזוהה ורגיש, וניהול קשר אינטראקטיבי עם נושאי המידע באמצעות הגופים ובאמצעות מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות הגנת הפרטיות (אבטחת המידע), שקיפות מול הלקוח, ומילוי החובות החלות מכח פרק הדיווח הישיר ושירותי הדיוור הישיר בחוק.

ממצאי הליך פיקוח הרוחב במגזר מועדוני הלקוחות מצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ ולאי עמידה בהוראות החוק בכל הנוגע למינויים של מנהלי מאגרים. בנוסף, נמצא כי מרבית מהגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את ציבור הלקוחות בדבר זכויותיו על פי חוק הגנת הפרטיות, הכוללות 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 תוכנית 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.

7%99%D7%93%D7%A2%20-%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

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית וממשל תאגידי			
אין כתבי מינוי של ממונה אבטחת מידע.	הוצאות כתב מינוי רשמי לממונה אבטחת מידע.	חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3	**מינוי ממונה אבטחת מידע**
אי עמידה בתכנית העבודה לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות.	עמידה בתכנית העבודה השנתית לנושא אבטחת המידע.	תכנית עבודה שנתית לבקרה שוטפת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
לא קיימת תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות.	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**
תכנית העבודה השנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות אינה מפורטת מספיק ואיננה כוללת את כל הרכיבים הנדרשים מתוכנית עבודה	עדכון תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות, כך שתכסה בצורה טובה את נושאי אבטחת מידע והגנה על הפרטיות ותפרט את הגורם האחראי ואבני דרך ברורים.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
מדיניות אבטחת מידע לא מעודכנת.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם.	נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נהלי אבטחת מידע**
העדר נהלי אבטחת מידע בחברה.	כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4,.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נהלי אבטחת מידע**
לא מבוצעות הדרכות לעובדים חדשים.	בהתאם להוראות התקנות, יש לבצע הדרכות לפני מתן או שינוי הרשאות גישה.	אבטחת מידע בניהול כוח אדם –הדרכת עובדים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(ב)	**הדרכות עובדים**
עובדי החברה בעלי גישה למאגרי המידע אינם עוברים הדרכות בנושא אבטחת מידע והגנת הפרטיות לפי החוק והתקנות או לא קיים תיעוד עבור הדרכות עובדים שבוצעו.	יש לקבוע הדרכות לפחות פעם בשנתיים במאגרים שחלה עליהם רמת האבטחה הבינונית או הגבוהה בנושא אבטחת מידע והגנת הפרטיות בצורה מספקת וניהול תיעוד ומעקב אחר הדרכות אלו.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(ג)	**הדרכות עובדים**
אין תהליך מיון לעובדים חדשים אשר בוחן היבטי פרטיות ואבטחת מידע	הטמעת תהליך מיון של עובדים חדשים שבוחן היבטים הרלבנטיים לפרטיות ולאבטחת מידע.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 7(א), תקנה 23	**מיון עובדים חדשים**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
אין התאמה בין מינוי מנהל המאגר בפועל לבין זה שנרשם אצל רשם מאגרי המידע.	עדכון והשלמת הרישום.	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות	**מינוי מנהל מאגר**
העדר עדכון ברשם אודות מינוי מנהל מאגר.	הסדרת רישום מנהל המאגר ברשם.	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות	**מינוי מנהל מאגר**
אי ביצוע ביקורת אבטחת מידע ו/או הגנת הפרטיות, אי ביצוע סקר סיכונים.	השלמת התהליך בהקדם וביצוע ביקורת בנושא אבטחת מידע וכן סקר סיכונים. 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.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5, תקנה 16	**ביקורות תקופתיות**
ניהול מאגרי מידע			
שימוש במידע שבמאגר המידע שלא למטרה שלשמה הוקם המאגר.	שימוש במידע שבמאגרי המידע בחברה ייעשה רק למטרה שלשמה הוקם מאגר המידע.	חוק הגנת פרטיות, תשמ"א-1981 סעיף 8 (ב)	**שימוש במידע בניגוד למטרה**
נוסח ההודעה ללקוח אינו עומד או עומד חלקית בדרישות סעיף 11.	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.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11	**מקור סמכות לאיסוף המידע**
לא ניתן לנושא המידע לעיין במידע אודותיו לפי בקשתו כנדרש בסעיף 13 לחוק במאגרי המידע.	מתן אפשרות לנושא המידע לממש את זכותו החוקית לעיון במידע אודותיו בהתאם לסעיף 13 לחוק, בכלל מאגרי המידע.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 13	**זכות העיון במידע**
נוסח ההודעה ללקוח באמצעות דיוור ישיר אינה כוללת את הפרטים הנדרשים בחוק.	ניסוח הודעה לכל פניה בדיוור ישיר אשר תכיל את הנושאים הבאים: 1. ציון כי הפניה היא בדיוור ישיר, בצירוף ציון מספר הרישום של המאגר המשמש לשירותי דיוור ישיר בפנקס מאגרי מידע; 2. הודעה על זכותו של מקבל הפניה להימחק מן המאגר, בצירוף המען שאליו יש לפנות לצורך כך; 3. זהותו ומענו של בעל מאגר המידע שבו מצוי המידע שעל פיו בוצעה הפניה, והמקורות שמהם קיבל בעל המאגר מידע זה.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 17 ג', 17 ד', 17 ה', 17 ו'	**דיוור ישיר ושירותי דיוור ישיר**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
אבטחת מידע			
תשתיות ומערכות חומרה לא נשמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה ובאופן שאינו תואם את אופי פעילות המאגר ורגישות המידע בו	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**
לא קיימים אמצעי הגנה מספקים אשר נותנים מענה לחדירה לא מורשית במאגרי המידע מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישה בתקנות.	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**
עדכון אנטי-וירוס מבוצע באופן שאינו מספק את דרישות התקנות	יש לפעול להגברת תדירות עדכון חתימות האנטי-וירוס	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 14 (א)	**אבטחת תקשורת**
לוגים אינם נשמרים לתקופה של לפחות 24 חודשים בהתאם לתקנות.	יישום מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (מנגנון הבקרה), ושמירת מעקב אודות נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 10	**בקרה ותיעוד גישה**
לא קיים תיעוד לגישה למאגרי מידע.	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	**בקרה ותיעוד גישה**
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	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	גיבוי ושחזור נתוני אבטחה תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 17 (ב) ותקנה 18	**גיבוי נתוני אבטחה**
בכניסה מרחוק למאגר על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	אופן הזיהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 14 (ג)	**גישה מרחוק**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא קיימת הפרדה בין מערכות מחשוב אשר ניתן מהן לגשת למידע, לבין מערכות מחשוב אחרות.	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**
מגבלה לחיבור התקנים ניידים לתחנות עבודה מהן ניתן לגשת למידע מהמאגר מידע לא כוללת הצפנה בעת העתקת המידע.	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**
במערכת לא מוטמעת מדיניות סיסמאות או לא קיימת מדיניות סיסמאות חזקה.	במאגרים בעלי רמת אבטחה בינונית ומעלה, קביעה בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכד'	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ב)	**מדיניות סיסמאות**
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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 9 (ג)	**ניהול הרשאות**
אין הפרדת תפקידים במערכות המידע של החברה.	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 8, תקנה 9 (א)	**ניהול הרשאות**
אי ביצוע ניתוק אוטומטי לאחר פרק זמן או ביצוע ניתוק אוטומטי לאחר פרק זמן לא סביר של אי 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)	**ניתוק אוטומטי**
לא נערך סקר סיכונים במהלך שלוש שנים האחרונות על ידי גורם מקצועי חיצוני בלתי תלוי במאגרי המידע בחברה.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים על ידי גורם חיצוני מקצועי ובלתי תלוי מידי אחת לשנה וחצי, בחינה את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ג)	**סקר סיכונים**
במאגר מידע שחלה עליו רמת האבטחה הגבוהה, לא נערכו מבדקי חדירה על ידי גורם מקצועי במאגרי המידע בחברה.	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.	מבדקי חדירות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 5(ד)	**מבדקי חדירה**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
אי עמידה בהוראות תקנה 11 בנוגע לתיעוד 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. 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**
עיבוד מידע אישי במיקור חוץ			
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.	תקנה 15 + הנחיות רשם מאגרי המידע מס' 2/2011	**מיקור חוץ**
נספח ההתקשרות עם הגורם החיצוני כולל סעיף כללי של עמידה בהוראות חוק הגנת הפרטיות, ללא התייחסות נדרשת לפעולות לביצוע, כנדרש בתקנות.	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 צד ג' בהעברת מידע לאחר.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15	**מיקור חוץ**
החברה אינה נוקטת פעולות בכדי לוודא שצד ג' נוקט באמצעים הנדרשים להגנת המידע	ווידוא כי כל גוף צד ג' אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15	**מיקור חוץ**