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 -

הגנת הפרטיות בקרב גופים המנהלים
פלטפורמות לימודיות וחינוכיות לקטינים





טבת תש"פ

ינואר 2020

תוכן עניינים

1. תקציר מנהלים 3
1.1. פיקוחים מגזריים 3
1.2. מגזר גופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים 3
1.3. תהליך העבודה 4
1.4. ליקויים, מסקנות והמלצות עיקריות 4
2. פלטפורמות לימודיות - תמונת מצב 6
2.1. כללי 6
2.2. רקע על המגזר 6
2.3. תהליך העבודה 7
2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו 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 11
4.1. בקרה ארגונית וממשל תאגידי 11
4.2. ניהול מאגרי מידע 11
4.3. אבטחת מידע 12
4.4. עיבוד מידע אישי במיקור חוץ 13
5. סיכום 14
נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם 15

1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות ("**הרשות**"), 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 והבהרות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות החוק.

1.1. פיקוחים מגזריים

במסגרת הליך פיקוח הרוחב בשנים 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 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 הגופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים, על אתגריו המיוחדים ומסקנותיו המגזריות. דוחות מסכמים נוספים על המגזרים הנ"ל מפורסמים באתר הרשות.[1]

1.2. מגזר גופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים

בשנת 2018 הרשות להגנת הפרטיות הגדירה את מגזר הגופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים (ובקצרה "**פלטפורמות לימודיות**"), כיעד פיקוח רוחב משמעותי בשל מאפייניו הייחודיים של מגזר זה. מאפיינים אלו כוללים בין היתר את פערי הכוחות המובנים במגזר זה בין הפלטפורמות הלימודיות האוספות את המידע לבין הקטין. מאפיין נוסף מתייחס לכך שהגופים במגזר זה מנהלים או מחזיקים מאגרי מידע רבים המתייחסים למידע אישי רגיש ומזוהה אודות קטינים ועבור קטינים, בגילי גן עד תיכון, לצרכים לימודיים שונים. פלטפורמות אלו אוספות מידע אישי על קטינים אשר נמסר על ידי מסגרות חינוכיות או בעת הרשמתו של הקטין לפלטפורמה הלימודית, וכן צוברות מידע נוסף בעת השימוש של הקטין בה, כגון ציונים, התקדמות לימודית, תמונות ועוד.

[1] ר' פעילות פיקוח הרוחב במחלקת האכיפה באתר הרשות להגנת הפרטיות:
https://www.gov.il/he/departments/general/enforcement_supervision

1.3. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב הרשות פנתה בדרישה למילוי שאלוני ביקורת ל-38 גופים המנהלים מידע אודות קטינים באמצעות פלטפורמות לימודיות.

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 ספקי פלטפורמות לימודיות עלה כי מרבית מהגופים שנבדקו נמצאו ככאלה שאינם מקפידים דיים ליידע את ציבור הקטינים על האופן שבו נאסף המידע אודותיהם, אינם מיידעים את הקטינים בצורה מספקת בדבר זכויותיהם מכוח חוק הגנת הפרטיות, כמו למשל, החובה להציג את מקור המידע והזכות לעיין במידע.

נמצאה רמת עמידה נמוכה בהוראות חוק הגנת הפרטיות בנוגע להסתייעות בשירותי מיקור חוץ לשם ביצוע פעולות לעיבוד מידע אישי הכולל בין היתר פרטי קשר, ציונים, שיוך למוסד חינוכי וכד'.

מרבית הגופים שנבדקו מחזיקים את מאגרי המידע בענן ובחוות שרתים שונות, המספקים שירותי אבטחת מידע שונים, דבר הגורם לגופים לייחס עמידה בתנאי האבטחה הנדרשים בחוק, בעוד שלמעשה נדרשת רכישה של שירותי אבטחה ספציפיים מחוות השרתים או נקיטת צעדי אבטחה עצמאיים באופן מקיף יותר, בכדי לעמוד בהוראות תקנות הגנת הפרטיות (אבטחת מידע).

בתחום של ניהול מאגרי מידע עלה פער משמעותי בין רמת עמידתם הגבוהה יחסית של גופים גדולים ממגזר זה בהוראות חוק הגנת הפרטיות והתקנות מכוחו לבין גופים קטנים אשר רמת עמידתם בהוראות החוק והתקנות נמצאה נמוכה יחסית.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 23 מתוך 24 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם. לאור בחינת כשלי המגזר, הרשות להגנת הפרטיות רואה חשיבות בפרסום דו"ח זה, על מנת שיהווה כלי עבודה מנחה, ויאפשר לגופים נוספים המנהלים מידע אודות קטינים לבצע הערכה עצמית ויגביר את המודעות לדרישות חוק הגנת הפרטיות בקרב גופים אלה. כך יוכלו הגופים בתחום לנהל את המידע של הקטינים בצורה מיטבית, תוך שמירה על זכויותיהם והגנה על פרטיותם.

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

דו"ח פיקוח רוחב 2018-2019

ממצאי הליך פיקוח הרוחב בקרב גופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים

טבת תש"פ, ינואר 2020

אתגרים ומאפיינים ייחודיים של המגזר

- השקיפות הנדרשת ממנהל המאגר בנוגע לזכויותיו של הקטין
- פערי כוחות בין מקבל המידע למוסר המידע
- ניהול מידע רגיש אודות קטינים הכולל בין היתר, חוות דעת על התנהגות ויכולות למידה, ציונים, הרגלי למידה, תמונות ועוד

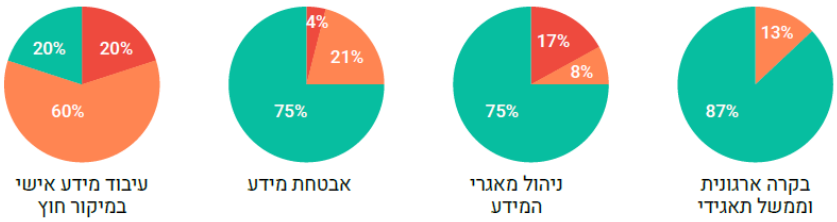
התהליך שבוצע במספרים

- **38** שאלונים שהופצו
- **24** גופים שנבדקו
- **11** דרישות להשלמת מידע חסר בכתב ובפיקוח בשטח
- **23** הנחיות לתיקון ליקויים

התנעה

פלטפורמות אינטרנטיות לימודיות המנהלות מידע אודות קטינים

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



עיקר הדרישות לתיקון הליקויים



- יש להעניק לקטין אפשרות לעיין ולבקש לתקן את המידע המצוי אודותיו במאגר.
- על הגופים האוספים מידע מקטינים להקפיד לשקף בפני הקטין את זכויותיו בעת קבלת ההסכמה ומסירת המידע על ידו, וכן בכל פנייה בדיוור ישיר, באופן בהיר וברור, כך שהסכמתו של הקטין למסירת המידע וזכויותיו תהיינה ברורות בהתאם לגילו ולהבנתו.
- יש לכלול בהסכמים עם ספקי מיקור החוץ את כלל הדרישות המנויים בתקנות הגנת הפרטיות (אבטחת מידע).
- מתן גישה כדרך קבע לגורם שלישי או העברתו למיקור חוץ, מהווה מסירת מידע למחזיק מאגר כאמור בהוראות החוק.
- יש לנקוט פעולות בכדי לוודא שמיקור החוץ נוקט באמצעים הנדרשים כדי להגן על מאגרי המידע.
- יש לקבוע נוהל אבטחת מידע לרבות מענה לכל הנושאים המנויים בתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, בהתאם לרמת האבטחה הנדרשת במאגר.
- יש לוודא ביטול הרשאות של עובד שסיים את תפקידו.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש להקפיד על ביצוע ניתוק אוטומטי לאחר פרק זמן סביר של אי פעילות.
- התחברות באמצעות שימוש באמצעי זיהוי חזקים כגון - קוד משתמש, סיסמה ואמצעי זיהוי נוסף.
- במערכות המחוברות לרשת האינטרנט, יש להקפיד על אמצעי הגנה מתאימים מפני חדירה לא מורשית ומפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.
- יש להכין הכנת תכנית לבקרה שוטפת על העמידה בדרישות תקנות הגנת הפרטיות (אבטחת מידע)
- קיום הליכי מיון לעובדים חדשים לצורך בחינת התאמתם לקבלת גישה למאגרי המידע.

2. פלטפורמות לימודיות - תמונת מצב

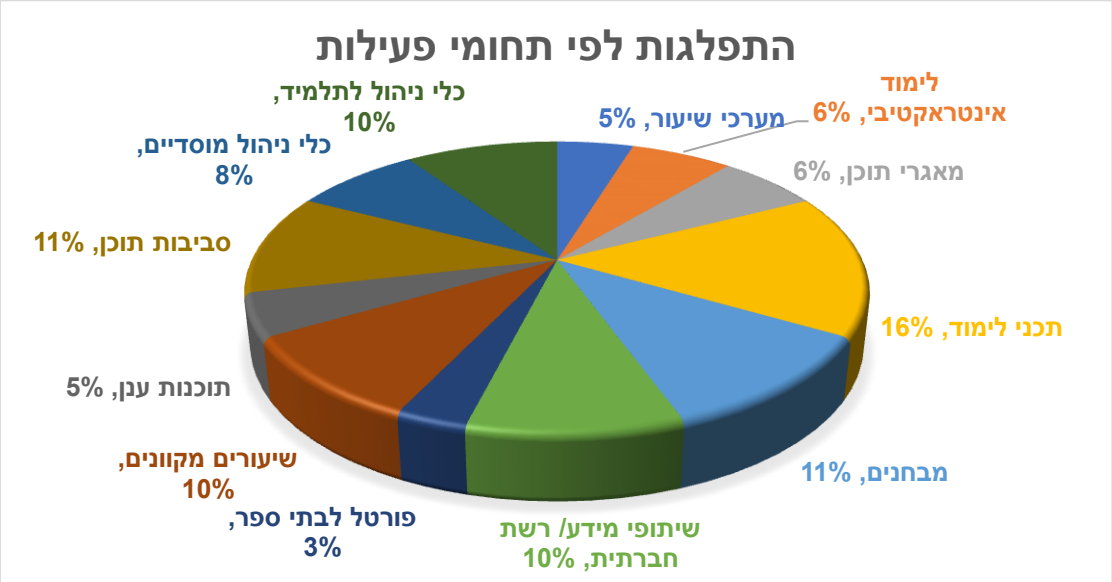
2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2018 לאוגוסט 2019 בגופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים.

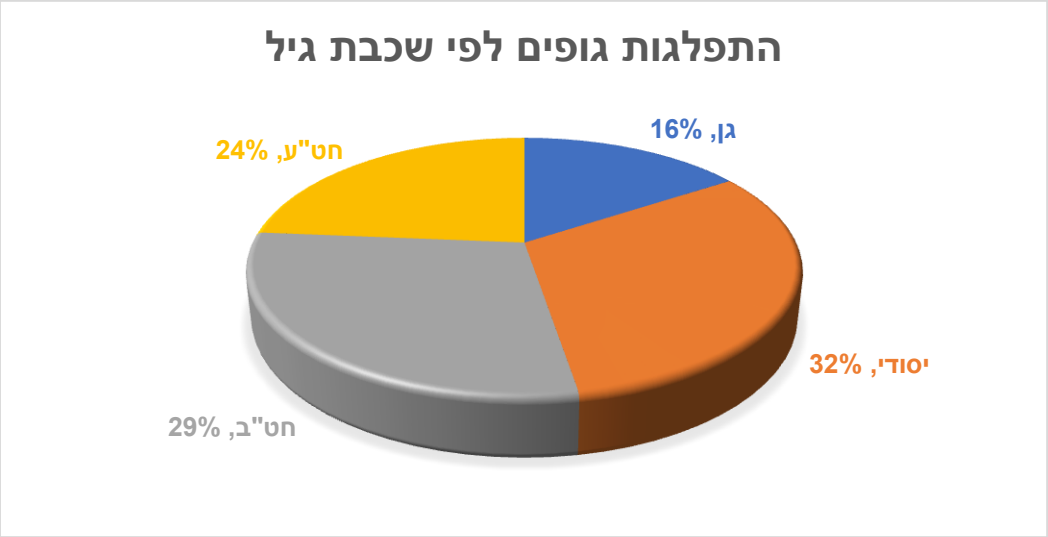
2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר ספקי פלטפורמות לימודיות, כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים. מדובר במגזר המספק פלטפורמות מקוונות המיועדות לקטינים, בגילי גן עד תיכון, לצרכים לימודיים כגון פורטלים חינוכיים המפרסמים מידע להורים ולתלמידים, אתרי שיעורים פרטיים, חוגים מקוונים, לימודי טכנולוגיה, מוזיקה ודת, פלטפורמות לימודיות חברתיות, הרגלי קריאה, שיתוף של תמונות ילדים ממסגרות חינוכיות וכד'. פלטפורמות אלו אוספות מידע אישי עם הרשמתו של הקטין או הוריו לפלטפורמה, וכן צוברות מידע נוסף בעת השימוש בה, כגון ציונים, התקדמות לימודית, תמונות ועוד. רגישות המידע ואופי נושאי המידע בקרב גופים אלו דורשים הקפדה מיוחדת על אבטחת המידע, קיום חובת השקיפות כפי שפורטה לעיל, ועמידה בהוראות החוק לעניין קבלת הסכמת נושא המידע ושקיפות בנוגע לשימוש במידע ועמידה בהוראות החוק בנוגע לדיווח ישיר ושירותי דיווח ישיר.

<u>התפלגות פעילות כלל הגופים המפוקחים, לפי תחומי פעילותם</u>



התפלגות שכבות הגיל הנכללים במאגרי הגופים המפוקחים



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.

השאלונים נשלחו ל- 38 גופים המנהלים פלטפורמות לימודיות, כאשר בניכוי גופים אשר סיימו פעילותם, שינו פעילות או דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, נמצאו תחת פיקוח 24 גופים. מתוכם 10 גופים נדרשו לספק מידע, מסמכים והבהרות נוספים לרשות, כאשר באחד מאותם הגופים הושלמו ואומתו ידיעות ומסמכים באמצעות פיקוח במשרדי הגוף המפוקח. בסיום ההליך נמצאו ליקויים ב-23 מתוך 24 גופים המפוקחים. בהתאם לכך, הורתה הרשות לאותם הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים, כאשר כחלק מההליך עשויה הרשות לבדוק בעתיד 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:

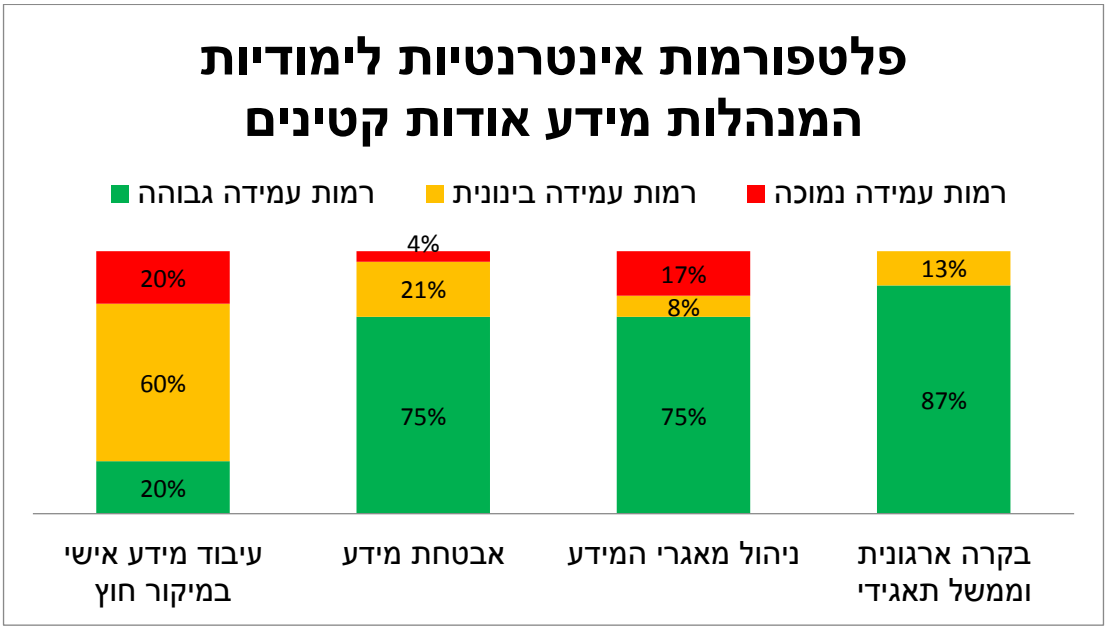
- **בקרה ארגונית וממשל תאגידי** - קריטריון זה בוחן קיומה של תכנית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;

- **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 (87%) נמצאה רמת עמידה גבוהה בהוראות החוק בנוגע לבקרה הארגונית וממשל תאגידי.[2]
- 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 גופים אשר אין להם תיעוד מסודר לנהלי אבטחת מידע ולתכנית עבודה שנתית או שהנהלים שהתקבלו אינם מספיק איכותיים בכך שאינם מקיפים את כלל הדרישות בהוראות התקנות.
- כמו כן, נמצאו גופים אשר טרם ערכו ביקורות בנושא אבטחת מידע/הגנת הפרטיות.

3.2. ניהול מאגרי מידע

- בתחום ניהול מאגרי מידע, נמצא כי 75% מהגופים עמדו בדרישות ברמה הגבוהה (מעל 80% עמידה), 8% ברמת הבינונית (בין 80-50%), ו17% ברמה נמוכה (מתחת ל50% עמידה), כאשר חלק מתוך אותם גופים שנמצאה בהם רמת עמידה נמוכה, היו כאלו אשר כמעט ולא עמדו בדרישות החוק כלל. פער זה בא לידי ביטוי בעיקר בין גופים גדולים ובינוניים שעמדו בדרישות ברמה גבוהה, לבין גופים הקטנים הפועלים במגזר זה., אשר טעו לחשוב כי אינם מנהלים או מחזיקים מאגר כהגדרתו בחוק כמפורט בהמשך.
- נמצאו ליקויים ביישום הוראות החוק בכל הנוגע לשקיפות בעת דרישת המידע ודבר מקור הסמכות לאיסוף המידע האישי, קל וחומר כאשר המדובר בקטינים, ויידוע הקטינים עליהם מוחזק המידע, בדבר זכויותיהם ובדבר מאגר המידע בו הם רשומים בעת פנייה בדיוור ישיר.
- מכלל גופים אלו, מרביתם לא הבהירו לקטינים את זכותם לעיין במאגרי המידע ולא ציינו זאת בתקנון שלהם או במסגרת אחרת.
- נמצאו גופים אשר לא אפשרו לנושאי המידע לשנות/לתקן את המידע המוחזק אודותיהם כנדרש בחוק.

3.3. אבטחת המידע

- במרבית הגופים (75%) נמצאה רמת עמידה גבוהה בהוראות החוק בנוגע לאבטחת מידע.[3]

[2] עמידה גבוהה זו מיוחסת בחלקה לדרישות המוטלות על גופים הפועלים במגזר זה כחלק ממתן שירותים לגופים חינוכיים. 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.

[3] ר' הערת שוליים 2

- מקרב הגופים שלא עמדו בצורה המיטבית בדרישות התקנות, נמצאו פערים בנושא אבטחת אמצעים נתיקים בין אם בהעדר הגבלות על שימוש באמצעים אלו או בהעדר הצפנה נאותה.
- כמו כן, נמצאו גופים אשר מנהלים מידע על קטינים, אשר במערכותיהם לא הותקנו אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.
- נמצאו גופים בעלי רמות אבטחה ברמה בינונית ומעלה אשר לא הגדירו במערכותיהם ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.
- נמצאו גופים אשר לא ערכו הליכי מיון של עובדים חדשים בעלי גישה למאגרי מידע/מערכות מאגר בטרם מתן הרשאות הגישה למידע בניגוד לדרישה בתקנות הגנת הפרטיות (אבטחת מידע).
- בחלק מהגופים לא ננקטו אמצעים לביטול הרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.
- נמצאו גופים אשר לא קבעו נוהל אבטחת מידע בהתאם למסמך הגדרות המאגר והתקנות, בהתאם לרמת האבטחה הנדרשת במאגר.

3.4. עיבוד מידע אישי במיקור חוץ

- הליקוי המרכזי שנמצא במגזר זה, מתייחס לקריטריון עיבוד מידע אישי במיקור חוץ, כאשר 80% מהגופים שנבדקו נמצאו ברמת עמידה בינונית ומטה (20% מהגופים בלבד נמצאו ככאלו העומדים בדרישות ברמה גבוהה, 60% ברמת עמידה בינונית, ו-20% נמצאו ברמת עמידה נמוכה).
- ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בארגון ועמדו באופן גבוה בדרישות החוק ובדרישות אבטחת המידע, נמצא עדיין ליקוי באופן יישום הדרישות מחברות צד ג' המעניקות שירותי עיבוד מידע אישי במיקור חוץ.
- ליקוי זה מתבטא בין היתר בכך שחלק מהגופים שנבדקו סברו בטעות שמתן הגישה כדרך קבע או העברתו למיקור חוץ אינה בגדר מסירת מידע למחזיק מאגר כאמור בהוראות החוק, וכתוצאה לא פעלו בהתאם לדרישות החוק בנושא זה.
- בנוסף, גם הגופים אשר ידעו כי הם מעבירים מידע למחזיק כהגדרתו בחוק, 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, לרבות קביעה במפורש בתנאי החוזה עם הגורם החיצוני, את התנאים והדרישות המתייחסות לסיכונים המפורטים בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע).
- מרבית מהגופים נמצאו ככאלה שלא 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 נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.

4. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר ספקי פלטפורמות לימודיות, הינם בעלי היכרות עם דרישות החוק והתקנות והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, וכי באופן כללי נמצאו עמידה גבוהה זו מיוחסת בחלקה לדרישות המוטלות על גופים הפועלים במגזר זה כחלק ממתן שירותים אותם הם מספקים לגופים חינוכיים. דרישות אלו נמצאו כמקיפות באופן חלקי בלבד בהיבטי הממשל הארגוני, ניהול מאגרי המידע ואבטחת המידע, בדגש על הגופים הגדולים הפועלים במגזר זה. עם זאת, עדיין נמצאו ליקויים משמעותיים באופן יישום הוראות החוק והתקנות, בכל הנוגע לאופן ההתקשרות של גופים אלו עם מיקור חוץ לצורכי עיבוד ואחסון המידע והנחיית הרשות היא כי על הגופים המשתייכים למגזר זה להקפיד על יישום החובות המוטלות עליהם בחוק, בתקנות ובהנחיות הרשות, בדגש על יישום הנקודות הבאות:

4.1. בקרה ארגונית וממשל תאגידי

נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, על הגופים גם 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 לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע).

4.2. ניהול מאגרי מידע

על הגופים המנהלים מאגרים הכוללים מידע כהגדרתו בחוק לבצע מיפוי לכל מאגרי המידע הקיימים אצלם. יובהר כי מידע הכולל נתונים כגון ציונים, לקויות למידה, הערכות על הישגים לימודיים וכד' הינו מידע אישי ואף עשוי להוות ה מידע רגיש כהגדרתו בחוק.

על הגופים לקבל 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 פערי הכוחות המובנים בין מבקש המידע לבין הקטין, על הגופים האוספים מידע מקטינים להקפיד על התאמת אופן השקיפות בפני הקטין בעת קבלת ההסכמה ומסירת המידע על ידו, באופן שיתאים לגילו ולהבנתו.

באותו מובן, על הגופים להקפיד גם בעניין דרישות החוק בינם לבין נושאי המידע הקטינים, בכל פנייה בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או באמצעי אחר, המהווה פנייה בדיוור ישיר כהגדרתה בסעיף 17ג' לחוק. גם בפניות אלו, על הגופים להקפיד על ציון הפרטים המנויים בסעיף 17ו' לחוק באופן המותאם לגילם והבנתם של נושאי המידע הקטינים - 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'.[4]

בנוסף, על הגופים להקפיד ליידע ולאפשר לנושאי המידע לעיין במידע שעליהם, 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.[5]

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 כי קיימים אצלם נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע), בהתאם למסמך הגדרות המאגר ורמת האבטחה הנדרשת, וכי נעשית בחינה של תוקפם מעת לעת כנדרש בתקנות.

על הגופים לוודא שקיימת תכנית עבודה שנתית העומדת בדרישות תקנות הגנת הפרטיות (אבטחת מידע), ולערוך אחת ל -24 חודשים לפחות ביקורת פנימית או חיצונית בנושא אבטחת מידע על ידי גורם בעל הכשרה מתאימה שאינו ממונה האבטחה של המאגר, כדי לוודא עמידה בתקנות.

על הגופים להקפיד על נקיטת אמצעים לביטול הרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

על הגופים לוודא כי במערכות החשופות לרשת האינטרנט, יותקנו אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב, וכי כל חיבור לאתר מאגר המידע אשר בעל רמת אבטחה בינונית ומעלה, נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, וכן לוודא כי מתבצע ניתוק אוטומטי לאחר פרק זמן של אי-פעילות, בהתאם לנדרש בתקנות הגנת הפרטיות (אבטחת מידע).

[4] 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

[5] 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

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.

על הגופים המחזיקים בתקן ISO 27001 לפעול בהתאם להנחיית 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.[6] 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 בפועל של הוראותיו לרבות כל הבקרות המפורטות בנספח A לתקן, באופן בו הן מפורשות בתקן.

4.4. עיבוד מידע אישי במיקור חוץ

בהתאם להוראות החוק, בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע. לפיכך, גוף המנהל מאגר חב באחריות על אבטחת המידע גם אם המידע מצוי במיקור חוץ לצורך עיבודו.

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, 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.[7]

עוד דורשות התקנות מן הגופים לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות. הוראות דומות לעניין החובות המוטלות על בעל

[6] 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

[7] 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

מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.[8]

5. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות קטינים, בקרב הגופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים, אשר נובעים מניהול מידע מזוהה ורגיש אודות הקטין, ונוכח פערי הכוחות המובנים בין מנהל ומחזיק המאגר לבין הקטין. פערים אלה דורשים הקפדה על יישום הוראות החוק והתקנות, באופן שיהא ברור לקטין בהתאם לגילו ולהבנתו.

כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות הגנת הפרטיות (אבטחת מידע), שקיפות מול נושאי המידע, ומילוי החובות החלות מכח פרק הדיווח הישיר ושירותי הדיווח הישיר בחוק.

ממצאי הליך פיקוח הרוחב במגזר ספקי פלטפורמות לימודיות 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, לאבטחת תקשורת ואי קביעת נהלי אבטחת מידע. בנוסף, נמצא כי מרבית הגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את נושאי המידע בדבר זכויותיהם על פי חוק הגנת הפרטיות, הכוללות בין היתר את החובה להציג את מקור המידע והזכות לעיין במידע.

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 הכוללת בין היתר, מחקר בנושא פרטיות תלמידים בעידן הדיגיטלי, ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות לפרסם את עמדתה בנוגע לדרכי הפעולה המיטביות של העוסקים בתחום זה, ולבחון את השינוי היחסי ברמת הציות להוראות החוק במגזרים השונים, על ידי בחינת גופים אחרים במגזרים אלה, 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 קיימת תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע.	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע 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 אינה מפורטת מספיק ואיננה כוללת את כל הרכיבים הנדרשים מתוכנית עבודה	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.	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**
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	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נהלי אבטחת מידע**
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**
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**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
ניהול מאגרי מידע			
נוסח ההודעה לקטין 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**
לא נמסרו לנושא המידע פרטים בדבר שימוש במאגר לדיוור ישיר או לשירותי דיוור ישיר	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**
המאגר אינו רשום אצל רשם המאגרים ולא דווחו פרטי מנהל מאגר כנדרש	יש לרשום את המאגר בפנקס המאגרים ברשות להגנת הפרטיות. יש למנות מנהל מאגר בטופס התואם לפירוט בטופס מינוי מנהל מאגר של הרשות להגנת הפרטיות	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 8, הגדרות	**רישום המאגר אצל רשם**
אבטחת מידע			
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**

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא מותקן אנטי וירוס בכל תחנה ושרת בארגון	יש לפעול להגברת תדירות עדכון חתימות האנטי-וירוס	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 14 (א)	**אבטחת תקשורת**
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 ברמה הבינונית והגבוהה 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**
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**
לא קיימת מגבלה לחיבור התקנים ניידים לתחנות עבודה מהן ניתן לגשת למידע מהמאגר המידע (חיבור דיסק און קיי או טלפון נייד) ולא ננקטו אמצעי הגנה מתאימים (כגון שיטות הצפנה מקובלות)	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**
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**

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**
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: 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 בהוראות ההסכם ובהוראות התקנות המפרטות את האמצעים הנדרשים להגנת המידע	ווידוא 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.	מיקור חוץ תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 15	**מיקור חוץ**