



דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר חברות
אחסון ועיבוד מאגרי מידע בישראל



חשוון תש"פ
אוקטובר 2020



3.....	1. תקציר מנהלים
3.....	1.1 פיקוחים מגזריים
3.....	1.2 מגזר חברות אחסון ועיבוד מאגרי מידע..... שגיאה! הסימניה אינה מוגדרת.
3.....	1.3 תהליך העבודה
4.....	1.4 ליקויים, מסקנות והמלצות עיקריות
6.....	2. חברות אחסון ועיבוד מאגרי מידע - 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 מכוח
8.....	3. ממצאים – ליקויים מרכזיים
8.....	3.1 בקרה ארגונית וממשל תאגידי
8.....	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
11.....	4.2 ניהול מאגרי מידע
11.....	4.3 אבטחת מידע
12.....	4.4 עיבוד מידע אישי במיקור חוץ
13.....	5. סיכום
15.....	נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

1. תקציר מנהלים

מערך פיקוח הרחוב ברשות להגנת הפרטיות ("הרשות") מופקד על עריכת פיקוחי רחוב מגזריים או נושאים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות" או "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות" או "תקנות 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. מגזר חברות אחסון ועיבוד מאגרי מידע

הרשות להגנת הפרטיות הגדירה את מגזר חברות אחסון ועיבוד מאגרי מידע בישראל כאחד מידי פיקוח הרחוב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה, המחזיק מאגרי מידע רבים המכילים מידע רגיש ומזוהה.

לעניין זה מגדיר החוק "מחזיק", לעניין מאגר מידע" - מי שמצוי ברשותו מאגר מידע דרך קבע והוא ראוי לעשות בו שימוש". הבחנה זו מתארת את החזקת המידע עבור אחרים, בעלי המאגר אשר מבקשים להשתמש בשירותיו של המחזיק כבעל היכולות הטכנולוגיות לאחסון ועיבוד המידע עבורם.

החברות בהן עסק הליך פיקוח הרחוב מעניקות שירותים שונים עבור בעלי מאגרי מידע שונים. בין היתר, שירותי תוכנה או פלטפורמה (Software as a Service - SAAS) - מאגר המידע הניתנים על-ידי מחזיק מאגר המידע המספק שירותים אלו, לרבות אירוח אתרי אינטרנט הכוללים מידע אישי. חלק מהחברות מעניקות שירותי תשתית (Infrastructure as a Service – IAAS), הכוללים מתן שירותי אחסון על ידי מחזיקים עבור בעלי המידע.

ניהול והחזקת מידע מחייבים את חברות אחסון ועיבוד המידע לעמוד בדרישות החלות על "מחזיקים" במידע כהגדרתם בחוק, אשר מחייבות אותם בין היתר לעמוד בדרישות אבטחת המידע, לקיים את חובת השקיפות אל מול הלקוח, ולעמוד בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר. כמחזיקים של מאגרים רבים, חלות על חברות האחסון ועיבוד המידע חובות נוספות לפי חוק הגנת הפרטיות הכוללות, בין היתר, מינוי ממונה על אבטחת מידע וחובת דיווח לרשות להגנת הפרטיות מדי שנה על המאגרים הנמצאים ברשותו, ניהול ההרשאות בהם, וציון שמם של בעלי המאגרים.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרחוב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל-36 גופים המנהלים שירותי אחסון ועיבוד מאגרי המידע. 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, בהתאם לרמת עמידתם בהוראות חוק הגנת הפרטיות והתקנות מכוחו.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר שירותי האחסון ועיבוד מאגרי המידע נמצא כי אין עמידה מספקת בהוראות החוק והתקנות על ידי גופים אשר מתוקף פעילותם מחזיקים ומעבדים מידע עבור אחרים.

חלק מהגופים הסיקו כי עליהם לדווח על מאגרים במסגרת SAAS בלבד, ונמנעו מלדווח על מאגרי מידע אחרים שברשותם, שאינם עולים כדי SAAS (כגון מאגרי PAAS – פלטפורמה כשירות, או IAAS – תשתית כשירות). אותם גופים סברו כי הוראות החוק אינן חלות בשירותי אחסון אחרים, שכן חברות האחסון אינן מתערבות בתכנים העולים לשרתיים. גישה זו אינה עולה בקנה אחד עם הגדרת "מחזיק" בחוק, וזאת לאור היכולת הטכנית לגשת למידע המאוחסן בשרתיים.

במרבית הגופים שנבדקו נמצאו חריגות במענה לדרישות התקנות, בחלקם אף חריגות משמעותיות. הליקויים הבולטים שנמצאו כללו בין היתר ליקויים בביצוע סקר סיכונים ומבחני חדירה בקרב חברות שהן בגדר בעלות מאגר מידע ברמת אבטחה גבוהה, וכן ליקויים בכל הנוגע לחובות החלות על נותן שירותי מיקור חוץ כפי שקבוע בהוראות תקנות אבטחת מידע, ובהנחיית רשם מאגרי המידע מס' 2/2011.

מהממצאים עולה כי אי העמידה בהוראות החוק והתקנות נובעת מכך שהגופים המעניקים שירותים כאמור אינם מודעים למלוא חובותיהם ביחס למידע המאוחסן אצלם עבור גופים אחרים בהיבטי תקנות אבטחת המידע.

לעניין זה, עמדת הרשות היא שחברה המספקת לאחר שירותי אחסון או גיבוי של מידע, לרבות בדרך של העמדת שרתים, נחשבת כ"מחזיקה" של המידע, גם אם תוכן המידע מוצפן והמפתח אינו מצוי בידיה אלא בידי בעל המאגר. מכאן, שעל החברות הפועלות במגזר זה ומעניקות שירותי אחסון או גיבוי, לרבות בדרך של העמדת שרתים, חלות כלל החובות לפי החוק והתקנות החלות על מחזיק במאגר מידע. הצפנת המידע המאוחסן והצפנת אופן העברתו אף שהינה חשובה מבחינת אבטחת המידע, אינה משחררת את המחזיק מאחריותו על פי הוראות החוק והתקנות.

לאור הממצאים שעלו מהליך פיקוח הרחב אשר הצביעו על כשל רחבי הדורש התייחסות כלל מגזרית, ונוכח הממצאים, מהם עלה כי הגופים הפועלים במגזר זה לא היו מודעים למלוא חובותיהם לפי החוק, מצאה הרשות לנכון לא לפנות באופן פרטני לגופים שנבדקו במגזר זה בנוגע לליקויים שנמצאו בנושא זה, אלא לפרסם במסגרת הדו"ח הבהרות והנחיות לכלל הגופים הפועלים במגזר, באשר לצעדים שעליהם לנקוט בכדי לעמוד בדרישות החוק והתקנות לתיקון הליקויים.

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל

חשוון תשפ"א אוקטובר 2020



דרגות שירות שונות באמצעות שירותי SAAS – Software as a Service, PAAS – Platform as a Service, IAAS – Infrastructure as a Service



ניהול מידע של מספר לקוחות על אותה פלטפורמה, היקפי המידע, ומספרם הרב של האנשים עליהם מוחזק המידע, דורשים הקפדה מיוחדת על עמידה בהוראות החוק והתקנות.

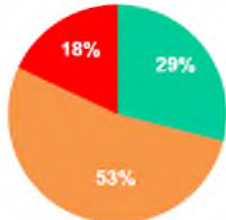


החזקת המידע נעשית עבור אחרים, המהווים בעלים של המאגר ומבקשים להשתמש בשירותיו של המחזיק, כבעל היכולות הטכנולוגיות לאחסון ועיבוד המידע עבורם.

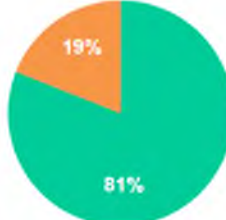


חברות המנהלות שירותי אחסון ועיבוד מאגרי מידע מחזיקות מאגרי מידע רבים הכוללים בין היתר מידע רגיש ומזוהה.

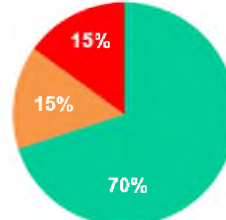
אתגרים ומאפיינים ייחודיים של מגזר חברות אחסון ועיבוד מאגרי מידע בישראל



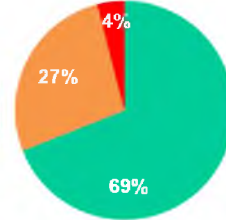
עיבוד מידע אישי במיקור חוץ



אבטחת מידע



ניהול מאגרי מידע



ביקורת ארגונית וממשל תאגידי

עמידה בהוראות חוק הגנת הפרטיות והתקנות מכוח

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

יש לוודא כי מונט כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע מקום שנדרש כזה.

יש לבצע הדרכות לבעלי הרשאות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סודיים.

יש לבצע ביקורת בנושא אבטחת מידע, סקר סיכונים ומבריק חדירות כנדרש בתקנות 5 ו-16 לתקנות אבטחת מידע.

יש לוודא קיום נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, וכי נעשית בחינה של תוקפם מעת לעת כנדרש בתקנות.

יש להבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה אך ורק למי שהורשו לכך במפורש בהסכם בכתב בינם לבין בעלי של אותו מאגר.

על גופים המחזיקים ברשותם חמישה מאגרי מידע או יותר, למנות אדם בעל הכשרה מתאימה כממונה על אבטחת מידע, ולמסור לרשם מדי שנה רשימה של מאגרי המידע שברשותם.

יש לוודא שקיימת תכנית עבודה שנתית העומדת בדרישות התקנות, 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 המחזיקים בתקן ISO 27001 לפעול בהתאם להנחיות רשם מאגרי המידע 3/2018 – 'תחולת תקנות הגנת הפרטיות (אבטחת מידע) על ארגונים המוסמכים לתקן ISO/IEC 27001.

יש לוודא את רישום כלל מאגרי המידע שבעלותם בהתאם להוראות החוק, וכן לוודא כי קיימת התאמה בין זהות מנהל המאגר במסמכי החברה, לבין הרישום אצל רשם מאגרי המידע.

על גופים המחזיקים ברשותם חמישה מאגרי מידע לפחות של בעלים שונים, למסור לרשם, מדי שנה, רשימה של מאגרי

המידע שברשותם, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על אבטחת המידע.

בדיוור ישיר, בין אם עבור לקוחות ישירים של הגופים ובין אם כפלטפורמה למתן שירותי דיוור ישיר יש להקפיד על ציון הפרטים המנויים בסעיף 117 לחוק.

החובות החלות על בעל מאגר מידע יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 15-1 (א) – הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.

על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, לבחון עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בה. יש לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, אשר יכלול את כל הוראות תקנה 15(א)(2) לתקנות וכן התייחסות לחובותיו ואחריותו של הספק הרבות: דיווח אודות אירועי אבטחת מידע, מנגנוני אבטחת מידע, שמירת המידע לאחר סיום תקופת ההתקשרות וחובות צד שלישי בהעברת מידע לאחר.

יש לוודא כי כל צד שלישי אשר מספק שירותי מיקור חוץ בתחום מאגרי המידע נקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי ביקורת ופיקוח.



2. חברות אחסון ועיבוד מאגרי מידע - תמונת מצב

2.1. כללי

הדו"ח המונח לפניכם, הינו הדו"ח המתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2018 ליוני 2019 במגזר חברות אחסון ועיבוד מאגרי מידע.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר שירותי אחסון ועיבוד מאגרי המידע כיעד פיקוח רחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר. חברות המנהלות שירותי אחסון ועיבוד מאגרי מידע מחזיקות מאגרי מידע רבים המתייחסים למידע רגיש ומזוהה.

לעניין זה מגדיר החוק "מחזיק, לעניין מאגר מידע" - מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". דהיינו, החזקת המידע יכולה להיות עבור אחרים, המהווים בעלים של המאגר ומבקשים להשתמש בשירותיו של המחזיק, כבעל היכולות הטכנולוגיות לאחסון ועיבוד המידע עבורם.

גופים אלו מעניקים שירותים שונים עבור בעלי מאגרי מידע שונים. חלק מהגופים מעניקים שירותי תוכנה או "שירות יישומים" (Software as a Service – SAAS) או פלטפורמה (Platform as a Service - PAAS), הכוללים אפליקציות, ממשקים ופיתוחים עבור בעלי מאגר המידע בשכבות שונות, הניתנים על-ידי המחזיק, לרבות אירוח אתרי אינטרנט הכוללים מידע אישי. גופים אחרים במגזר זה מעניקים שירותי תשתית (Infrastructure as a Service – IAAS), הכוללים מתן תשתיות לרבות שירותי אחסון והעמדת שרתים בלבד.

ניהול מידע של מספר לקוחות על אותה פלטפורמה, היקפי המידע, ומספרם הרב של האנשים עליהם מוחזק המידע, דורשים הקפדה מיוחדת על עמידה בהוראות החוק והתקנות. בין היתר, נדרשות חברות האחסון לעמוד בקפדנות על דרישות אבטחת המידע, לקיים את חובת השקיפות אל מול הלקוח, ולעמוד בהוראות החוק גם בכל הנוגע לחובותיהם הנוספות כמחזיקות של מספר מאגרי מידע, ובכלל זה החובה למנות ממונה אבטחת מידע ולדווח לרשות מדי שנה על מצב מאגרי המידע, ואופן ניהולם.

2.3. תהליך העבודה

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, והינו חלק מתוכנית העבודה הכללית של הרשות. ראשיתו של התהליך ביצירת סקר הסיכונים לפרטיות שעורכת הרשות, לאיתור המגזרים והתחומים בהם היא מתכוונת לעסוק; בניית תכנית עבודה שנתית הכוללת תהליך של מחקר מדיניות, פרסום, הדרכה ותוכנית אכיפה שנתית, אשר במסגרתה נבחרים מגזרי פיקוח הרוחב. בחירת המגזרים והחברות שייבדקו נעשית בהתחשב בכמות והיקף המידע במגזר, ברמת רגישות המידע, ובידע



שהצטבר ברשות בנוגע למגזר והצורך בבחינה מגזרית והנחייתו לשם הבאתו לרמת עמידה נאותה בדרישות החוק.

במסגרת הפעילות במגזר זה, נשלחו שאלונים ל- 36 גופים המנהלים שירותי אחסון, או אחסון ועיבוד מאגרי מידע. בניכוי הגופים אשר סגרו את פעילותם, שינו אותה או דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, ולאחר שאוחדו גופים אשר השיבו מענה מאוחד בשל פעילות עסקית מאוחדת או ניהול שימוש במאגר או תשתית טכנולוגית משותפת, נותרו בהליך הפיקוח 26 גופים.

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

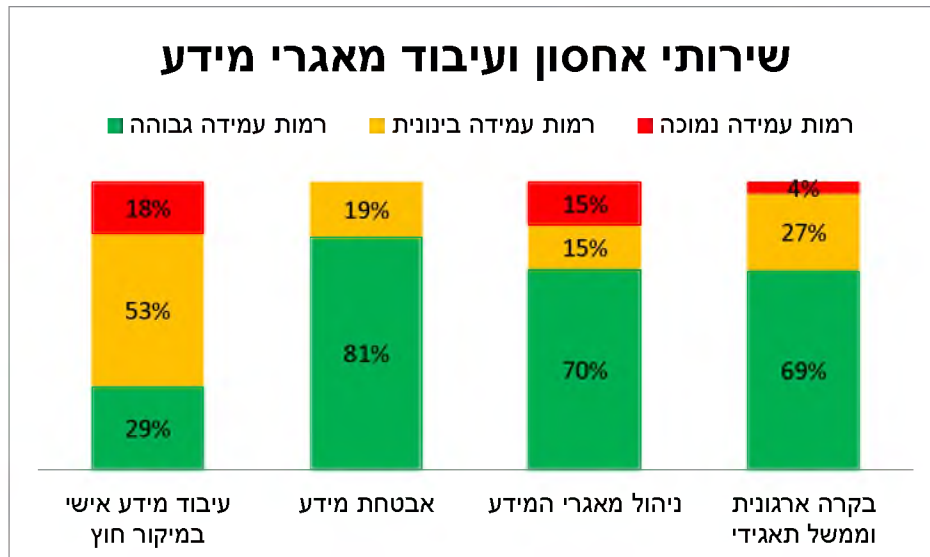
במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת, הבוחנים ארבעה קריטריונים עיקריים:

- **בקרה ארגונית וממשל תאגידי** - בחינת קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות, ומינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** - בחינת אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה לשמה נאסף, מתן זכות העיון במידע, ועמידה בהוראות החוק בעניין דיוור ישיר;
- **אבטחת מידע** - בחינת עמידת הגופים בהוראות תקנות אבטחת מידע, בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם;
- **שירותי מיקור חוץ** - בחינת ההתקשרויות של בעלי מאגרי המידע עם גורמים חיצוניים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע.

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

- 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 ואת ההנחיות שניתנו לתיקון הליקויים לגופים הספציפיים, ניתן למצוא בנספח א' להלן.

3.1. בקרה ארגונית וממשל תאגידי

- במרבית הגופים (69%) נמצאה רמת עמידה גבוהה בהוראות החוק בנוגע לבקרה הארגונית וממשל תאגידי¹.
- עם זאת, אצל כשליש מהגופים (31%), נמצאה רמת עמידה בינונית ומטה באופן ניהול הבקרה הארגונית והממשל התאגידי. בין היתר נמצאו גופים מפוקחים אשר מינו בעלי תפקידים ללא כתב מינוי ועדכון בפנקס מאגרי המידע כנדרש בחוק.
- נמצאו בעלי מאגרי מידע שחלה עליהם רמת אבטחה גבוהה, אשר נדרשו לבצע ביקורות אבטחת מידע או מבדקי חדירות אשר לא בוצעו כנדרש או לא בוצעו כלל.
- עוד נמצאו גופים אשר לא ניהלו תיעוד עבור הדרכות ריענון לעובדים בעלי גישה למאגרי מידע/מערכות מאגר.

3.2. ניהול מאגרי מידע

- בתחום ניהול מאגרי מידע, נמצא כי 70% מהגופים עמדו בדרישות ברמה גבוהה (קרי, מעל 80% עמידה); 15% ברמת בינונית – עמידה חלקית בהוראות החוק; ו- 15% ברמה נמוכה – אי עמידה במרבית או בכל הוראות החוק והתקנות².

¹ עמידה גבוהה זו מיוחסת בחלקה למסגרת השירותים הניתנים על-ידי גופים אלו ללקוחות, בדומה לרמת עמידה גבוהה יחסית באופן ניהול מאגרי המידע ואבטחת המידע אשר ניתן לייחס למסגרת הטכנולוגית בה פועל מגזר זה והשימוש במערכות טכנולוגיות בעלות רמות אבטחת מידע נאותות. עם זאת, רמות העמידה בהוראות החוק והתקנות נמצאו כלא מספקות בכל הנוגע לאופן ההתקשרות של גופים אלו כגורמי מיקור חוץ או בשימוש של גופים אלו במיקור חוץ לצורכי עיבוד ואחסון המידע.

² עמידה גבוהה זו מיוחסת בחלקה בנוסף לאמור בהערת שוליים 1 גם לדרישות המוטלות על גופים הפועלים במגזר זה כחלק מדרישת הלקוחות בקבלת השירותים.



- בין הגופים בהם נמצאה רמת עמידה חלקית, אשר מבצעים פניות בדיוור ישיר בעצמם או עבור אחרים, נמצאו ליקויים ביישום הוראות החוק בכל הנוגע לשקיפות בדבר מקור הסמכות לאיסוף המידע האישי, ויידוע האנשים עליהם מוחזק המידע בדבר זכויותיהם בנוגע למאגר המידע בו נשמרים פרטיהם.

3.3. אבטחת המידע

- במרבית הגופים (81%) נמצאה רמת עמידה גבוהה בהוראות החוק בנוגע לאבטחת מידע.³
- נמצאו גופים בעלי רמת אבטחת מידע בינונית ומעלה לגביהם, בכניסה למאגר המידע באמצעות רשת האינטרנט, לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
- מקרב הגופים שלא עמדו בצורה המיטבית בדרישות התקנות, 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, גופים בעלי תקן ISO27001 סברו שקיום התקן מספק את הדרישות בתחום אבטחת המידע, בניגוד להנחיית רשם מאגרי המידע מס' 03/2018 הקובעת כי עמידה בתקן מהווה ראיה לעמידה בחלק מהוראות התקנות בלבד, ובתנאים מסוימים.
- עוד נמצאו גופים אשר אינם מקיימים תיעוד וקביעת הוראות התמודדות עם אירועי אבטחת מידע כנדרש בתקנות.

3.4. עיבוד מידע אישי במיקור חוץ

- הליקוי המרכזי שנמצא במגזר זה מתייחס לקריטריון עיבוד מידע אישי במיקור חוץ, כאשר 71% מהגופים שנבדקו הראו עמידה חלקית בהוראות החוק או אי-עמידה כלל (18% מהגופים נמצאו ברמת עמידה נמוכה, ו-53% ברמת עמידה בינונית).
- ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בארגון, קיים עדיין ליקוי ביישום הדרישות מחברות חיצוניות המעניקות שירותי עיבוד מידע אישי במיקור חוץ. ליקוי זה מתבטא בכך שהגופים בהם נמצאה רמת עמידה בינונית או נמוכה, לא נקטו צעדים מספקים מבעוד מועד על מנת להעריך את מידת הסיכון הנשקפת למידע, ולפגיעה אגב כך בזכותם לפרטיות של נושאי המידע, כפועל יוצא מהשירותים הניתנים על ידם במיקור חוץ, או בשימוש של הגופים עצמם במיקור חוץ בכל הנוגע לעיבוד ואחסון מידע.
- בין היתר נמצא כי חלק מהגופים אינם מבצעים התקשרות לפי תקנה 15 לתקנות אבטחת מידע בצורה מספקת, אינם בוחנים את איכות ניהול אבטחת המידע ואופן

³ ר' הערת שוליים 1



תפעול מאגרי המידע אצל ספקי מיקור החוץ, ואינם מבצעים פעולות פיקוח כנדרש.

4. מסקנות/תמונת מצב והמלצות

ממצאי הליך פיקוח הרחב עולה כי חלק מהגופים הסיקו כי עליהם לדווח על מאגרים במסגרת SAAS בלבד, ונמנעו מדווח אודות מאגרי מידע נוספים שברשותם.

במסגרת זו יש להבהיר כי חברה הנותנת שירותי אחסון לרבות בדרך של העמדת שרתים,⁴ נחשבת כ"מחזיקה" של המידע כהגדרת "מחזיק" בחוק, גם אם תוכן המידע מוצפן והמפתח אינו מצוי בידיה אלא בידי בעל המאגר. על חברה המציעה שירותי אחסון ועיבוד מאגרי מידע לברר במהלך ההתקשרות למתן שירותים, האם במסגרת השירות נדרשת החזקה במידע כהגדרתו בחוק, ככל שלא ניתנה מצד בעל המידע הפוטנציאלי הצהרה בדבר העדר מידע, חזקה על נותן השירות כי הינו מחזיק במאגר מידע.

במרבית הגופים שנבדקו נמצאו חריגות במענה לדרישות התקנות, בחלקם אף חריגות משמעותיות באופן יישום הוראות החוק והתקנות. הנחיית הרשות היא כי על הגופים המשתייכים למגזר זה ליישם את ההיבטים הבאים:

4.1 בקרה ארגונית וממשל תאגידי

נוכח הליקויים שנמצאו בקריטריון זה, על הגופים לוודא 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 מקום שנדרש כזה, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות אבטחת מידע.

כמו כן, בהתאם להוראות התקנות, יש לבצע הדרכות לגורמים האמורים אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. תיעוד לחומרים שהועברו וכן תיעוד לביצוע ההדרכות – יישמר.

בנוסף, על הגופים לפעול להשלמת התהליך בהקדם וביצוע ביקורת בנושא אבטחת מידע, סקר סיכונים ומבדק חדירות כנדרש בתקנות 5 ו-16 לתקנות אבטחת מידע.

⁴ כאשר מדובר בשירות תשתית אשר אינו כולל שירותי אחסון או העמדת שרתים ללקוח. יחולו אך ורק החובות המתייחסות לחובות האבטחה בהיבטי האבטחה הפיסית של המתקן של נותן השירות.



4.2. ניהול מאגרי מידע

החובה המוטלת מכוח החוק על הגופים המנהלים רשימת לקוחות המהווה מידע כהגדרתו בחוק, כוללת את הצורך לבצע מיפוי לכל מאגרי המידע הקיימים אצלם. על בסיס מיפוי זה עליהם לרשום מאגרי מידע שאינם רשומים או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

כמו כן, על הגופים לקבל את הסכמת נושא המידע כנדרש בחוק לצורך שמירת פרטיו במערכת הארגון (באמצעות פניה לנושא המידע לפי סעיף 11 לחוק).

על גופים המחזיקים ברשותם חמישה מאגרי מידע לפחות של בעלים שונים, למסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותם, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על אבטחת המידע.

בכל הנוגע לפניות בדיוור ישיר, בין אם עבור לקוחות ישירים של הגופים ובין אם כפלטפורמה למתן שירותי דיוור ישיר - בכל פנייה בכתב, בדפוס, בטלפון, בפקס, בדוא"ל או באמצעי אחר, המהווה פנייה בדיוור ישיר כהגדרתה בסעיף 17 לחוק, על הגופים להקפיד על ציון הפרטים המנויים בסעיף 17 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 ועוד.

4.3. אבטחת מידע

סעיף 17 לחוק קובע כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

על הגופים הפועלים במגזר זה, לעמוד בכל הוראות החוק והתקנות הן בהיותם בעלי מאגרי מידע והן מתוקף היותם מחזיקים לענין החוק, המעניקים שירותי מיקור חוץ לעיבוד ואחסון מידע עבור אחרים.

בין יתר הליקויים שנמצאו בנושא ניהול הרשאות במאגרי המידע של גופים במגזר זה, ובהתאם להוראות תקנות אבטחת מידע, על הגופים לוודא כי קיימים אצלם נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, וכי נעשית בחינה של תוקפם מעת לעת כנדרש בתקנות.

על הגופים המחזיקים מאגרי מידע עבור בעלי מאגר שונים, להבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה אך ורק למי שהורשו לכך במפורש בהסכם בכתב בינם לבין בעליו של אותו מאגר. בנוסף, ככל שהגופים מחזיקים ברשותם חמישה מאגרי מידע או יותר, עליהם למנות אדם בעל הכשרה מתאימה כממונה על אבטחת מידע, ולמסור לרשם מדי שנה רשימה של מאגרי המידע שברשותם, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על אבטחה המידע.

על הגופים לוודא שקיימת תכנית עבודה שנתית העומדת בדרישות התקנות, 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 לוודא כי במערכותיהם החשופות לרשת האינטרנט יותקנו אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב, וכי בכל גישה למאגר מידע אשר הינו בעל רמת אבטחה בינונית ומעלה, ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, וכן לוודא כי מתבצע ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.

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

על הגופים 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 התקנות בנוסף לעמידה מלאה בתקן.⁵ הרשות רואה ארגון כמי שמקיים את הוראות התקנות במלואן ביחס למאגרים עליהם ניתנה הסמכה לתקן וכל עוד ההסמכה עומדת בתוקפה בהתקיים שני תנאים מצטברים: עמידה בכלל התקנות המפורטות בהנחיה וקיום הוראות התקן לרבות כל הבקורות המפורטות בנספח A לתקן, באופן בו הן מפורשות ומפורטות בתקן ISO/IEC 27002:2013(E).

על הגופים לוודא שבכניסה לאתר מאגר המידע, נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, עמידה בתנאי תקנה 9 (ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, לפי תקנה 11 לתקנות.

4.4. עיבוד מידע אישי במיקור חוץ

בקריטריון זה יודגש כי מגזר חברות האחסון ועיבוד מאגרי מידע כפוף לדרישות החוק והתקנות בשני תפקידים – האחד מתוקף היותו נותן שירותים אלו כספק מיקור חוץ, והשני כמי שמקבל שירותים דומים בעצמו.

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 התקנות 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



בהתאם לתקנה 19 לתקנות, החובות החלות על בעל מאגר מידע יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 2 ו-15(א) – הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.

בנוסף, בהתאם לתקנה 15 על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בה. בנוסף, על הגופים בעלי המאגר לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הוראות תקנה 15(א)(2) לתקנות, לרבות חובות 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.⁶

5. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות לקוחות בקרב מגזר שירותי אחסון ועיבוד מאגרי מידע, אשר נובעים מניהול מידע רב באמצעות הגופים ובאמצעות מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות התקנות, שקיפות מול הלקוח, ומילוי החובות החלות מכוח פרק הדיוור הישיר (סעיפים 17ג-17ט) בחוק.

ניכר כי קיימת אי בהירות באשר להיקף תחולת החוק והתקנות על כלל הגופים המסתייעים למגזר זה, מתוקף היותם מחזיקים במאגר מידע. לאור ממצאים אלו אשר הצביעו על כשל רחבי הדורש התייחסות כלל מגזרית ונוכח חוסר מודעות חלק ניכר מהגופים הפועלים במגזר זה למלא חובותיהם לפי החוק, מצאה הרשות לנכון שלא לפנות באופן פרטני לגופים שנבדקו בנוגע לליקויים שנמצאו.

לפיכך מבהירה הרשות לכלל הגופים הפועלים במגזר זה, כי **חברה המספקת לאחר שירותי אחסון או גיבוי של מאגר מידע לרבות בדרך של העמדת שרתים, נחשבת כ"מחזיקה" במאגר המידע, גם אם תוכן המידע מוצפן והמפתח אינו מצוי בידיה אלא**

⁶ לקריאה נוספת ר' הנחיית רשם מאגרי המידע 2/2011 – שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי -

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



בידי בעל המאגר. כפועל יוצא מכך, חלות עליה כלל החובות לפי החוק והתקנות החלות על מחזיק מאגר מידע. הצפנת המידע המאוחסן והצפנת אופן העברתו אף שהינה חשובה מבחינת אבטחת המידע, אינה משחררת את המחזיק מאחריותו על פי הוראות החוק והתקנות.

ממצאי הליך פיקוח הרחב במגזר שירותי אחסון ועיבוד מאגרי מידע מצביעים גם על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ ותיעוד אירועי אבטחה. בנוסף, נמצא כי מרבית הגופים 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 הרחב עורר אצל המפוקחים תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי ומחזיקי מאגרי מידע אישי באמצעות פיקוחי הרחב, 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 הרחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזרים השונים, על ידי בחינת גופים אחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

נושא	הפניה לחוק/תקנה/הנחיה	פעילות מתקנת נדרשת	הליקוי/פער
בקרה ארגונית וממשל תאגידי			
מינוי ממונה אבטחת מידע	סעיף 17ב' לחוק הגנת פרטיות, תשמ"א-1981. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3	יש לפעול למינוי ממונה על אבטחת המידע.	בגוף המחויב במינוי ממונה אבטחת מידע על פי החוק, לא מונה ממונה אבטחת מידע.
מינוי ממונה אבטחת מידע	סעיף 17ב' לחוק הגנת פרטיות, תשמ"א-1981. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3	יש למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחת הכפוף ישירות למנהל המאגר.	בגוף המחויב במינוי ממונה אבטחת מידע על פי החוק, אין למנות מנמ"ר כממונה אבטחת המידע.
ביקורות תקופתיות	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, סעיף 16	עריכת ביקורות בנושא אבטחת מידע/הגנת הפרטיות מדי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה. עריכת סקר סיכונים מדי 18 חודשים במאגר ברמת אבטחה גבוהה, הכולל את דרישות הביקורת.	לא בוצעה ביקורת אבטחת מידע.
הדרכות עובדים	אבטחת מידע בניהול כוח אדם – הדרכת עובדים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 7.	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.	לא קיים תיעוד עבור הדרכות עובדים שבוצעו
מינוי מנהל מאגר	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות	יש למנות מנהל למאגר המידע. ולעדכן את רשם מאגרי המידע בהתאם.	לא מונה מנהל מאגר.
מינוי מנהל מאגר	פרטי מנהל המאגר חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות	הסדרת רישום מנהל המאגר ברשם.	אין התאמה בין מנהל המאגר כפי שדווח על ידי החברה ומנהל המאגר כפי שמופיע ברשות.

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
לא קיימים נהלי אבטחת מידע.	כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.	נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4	נהלי אבטחת מידע
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 ברורות.	תכנית עבודה שנתית לבקרה שוטפת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3 (3)	תכנית עבודה
ניהול מאגרי מידע			
לא מבוצע דיווח שנתי לרשם מאגרי המידע על ידי מחזיקים בחמישה מאגרים ומעלה	על גופים המחזיקים ברשותם חמישה מאגרי מידע לפחות של בעלים שונים, למסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותם, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על אבטחת המידע	דיווח מחזיקים חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 17א' (ב)	דיווח מחזיקים
לא ניתן לנושא המידע לתקן את המידע אודותיו לפי בקשתו כנדרש בסעיף 14 לחוק.	יש לאפשר לנושא המידע לעדכן את המידע שאינו נכון/שלם/ברור או מעודכן האגור אודותיו בכל מאגרי המידע.	זכות נושא המידע לבקש לתקן את המידע. חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 14	זכות לעיון/תיקון במידע
לא נמסרת לנושאי המידע הודעה המפרטת לשם מה מבוקש המידע, למי יימסר המידע ומטרות המסירה.	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.	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 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
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.	יש לוודא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב במאגר המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת בהתאם לדרישות התקנות.	אבטחת תקשורת תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (א)	אבטחת תקשורת
לא מתבצע עדכון חתימת אנטי-וירוס	יש לפעול להגברת תדירות עדכון חתימות האנטי-וירוס	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (א)	אבטחת תקשורת
לא מנוהל מנגנון תיעוד אוטומטי שמאפשר 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.	יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של הניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.	בקרה ותיעוד גישה תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 10	גישה מרחוק
לא קיימת הפרדה בין מערכות מחשוב אשר ניתן מהן לגשת למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	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

נושא	הפניה לחוק/תקנה/הנחיה	פעילות מתקנת נדרשת	הליקוי/פער
התקנים ניידים והצפנה	התקנים ניידים תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 12	יש לבצע הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.	קיימת מגבלה חלקית בחיבור התקנים ניידים ללא שימוש במנגנוני הצפנה.
מדיניות סיסמאות	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב)(2)	במאגרים בעלי רמת אבטחה בינונית ומעלה, קביעה בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכד'.	במערכת לא מוטמעת מדיניות סיסמאות או לא קיימת מדיניות סיסמאות חזקה.
ניהול הרשאות	ניהול הרשאות תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 8, תקנה 9 (א)	יש להטמיע מנגנון הרשאות המבוסס על "הצורך לדעת" ולוודא תקופתית כי הרשאות הגישה הקיימות לעובדים תואמות עיקרון זה.	לא נמסר תיעוד מבסס לקיום הפרדת תפקידים במערכות המידע של החברה
ניהול הרשאות	זיהוי ואימות בעת התחברות למאגר מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ג)	אפיון ויישום תהליך בו מיד בעת סיום תפקיד או עזיבת עובד הארגון, הרשאותיו של העובד יבוטלו או יעודכנו בהתאם לצורך.	לא קיים תהליך לביטול הרשאות לבעל הרשאה שסיים את תפקידו או מנגנון לעדכון הרשאות לבעל הרשאה שעבר לתפקיד חדש, או שאינו מתקיים בסמוך לשינוי סטטוס העובד.
תיעוד אירועי אבטחה	תיעוד של אירועי אבטחה תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 11	יש לתעד כל אירוע המעלה חשש לאירוע אבטחה, בנוסף נוהל העבודה יכול 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.	לא קיים הליך סדור לתיעוד וקביעת הוראות התמודדות עם אירועי אבטחת מידע
עיבוד מידע אישי במיקור חוץ			



הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
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 גורם חיצוני 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
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
אי נקיטת פעולות בכדי לוודא שהגוף החיצוני נוקט בהוראות ההסכם ובהוראות התקנות המפרטות את האמצעים הנדרשים להגנת המידע	ווידוא כי כל גוף חיצוני אשר נותן שירותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15	מיקור חוץ