דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר קופות גמל וקרנות השתלמות



תוכן עניינים

1.תקציר מנהלים..... 3

1.1.מגזר קופות גמל וקרנות השתלמות..... 3

1.2.תהליך העבודה..... 4

1.3.ליקויים, מסקנות והמלצות עיקריות..... 4

2.פיקוח קופות גמל וקרנות השתלמות - תמונת מצב..... 6

2.1.כללי..... 7

2.2.רקע על המגזר..... 7

2.3.תהליך עבודה..... 8

2.4.הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו..... 9

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות: 10

3.1.בקרה ארגונית..... 11

3.2.ניהול מאגרי מידע ועיבוד מידע אישי במיקור חוץ..... 13

3.3.אבטחת מידע..... 14

4.מעקב תיקון ליקויים 17

5.סיכום..... 18

1. תקציר מנהלים

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

1.1. מגזר קופות גמל וקרנות השתלמות

בשנת 2020 הרשות להגנת הפרטיות הגדירה את מגזר קופות גמל וקרנות השתלמות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה בהיבטי הפרטיות, הבאים לידי ביטוי בהיבטים הבאים:

1. רגישות המידע המנוהל – ניהול נתונים אישים של עמיתים (מידע רפואי, כלכלי, דמוגרפי, קשרים משפחתיים וכד').
2. ניהול מידע אודות עמיתים שהינם חולים ועמיתים שנפטרו (לצורך קביעת קצבת נכות / קצבת שארים וכדו').
3. ניהול המידע אודות העמיתים מחייב את אותם ארגונים לעמוד בדרישות אבטחת המידע, כולל הסדרת נהלי עבודה בתחום אבטחת המידע והתמודדות עם אירועי אבטחת מידע, וכן מתן מידע בהתאם להוראות החוק והתקנות לנושא המידע לצורך שמירתו במאגר.

1.2. תהליך העבודה

בהליך פיקוח הרוחב במגזר זה, פנתה הרשות לקופות גמל וקרנות השתלמות בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע ורגישות המידע הנאסף. הליך הפיקוח החל ב-51 גופים, במגזר קופות גמל וקרנות השתלמות, שנבחרו על ידי הרשות, כאשר בניכוי גופים אשר פעילותם מוזגה, וגופים אשר הצהירו שאינם מחזיקים מאגר מידע, נותרו תחת הפיקוח 48 גופים. במהלך הפיקוח נדרשו 25 גופים לספק מידע, מסמכים והבהרות נוספות לרשות, כאשר נוכח משבר נגיף הקורונה, הוחלט לבצע השלמות ואימות ידיעות ומסמכים באמצעות פיקוח בפגישה מקוונת באחד הגופים המפוקחים. בסיום ההליך, נמצאו בכל 48 הגופים המפוקחים ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר קופות גמל וקרנות השתלמות נמצאה רמת עמידה גבוהה יחסית בהוראות חוק הגנת הפרטיות והתקנות, כאשר בשקלול הציונים שניתנו לגבי מידת העמידה בהוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 79%. נוכח הממצאים שעלו מהליך פיקוח הרוחב, קיבלו כל הגופים שנבדקו (48 מתוך 48) הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

ממצאי הליך פיקוח רוחב
בקרב מגזר קופות גמל וקרנות השתלמות

דו"ח פיקוח רוחב 2019-2020

אתגרים ומאפיינים ייחודיים של מגזר קופות גמל וקרנות השתלמות

במגזר קיימים שלושה סוגי תאגידים עיקריים:
1. קופות גמל וקרנות השתלמות ענפיות /מפעליות/סקטוריאליות (למגזרים מסוימים, עובדי סקטור או מפעל מסוים)
2. קופות גמל וקרנות השתלמות כלליות (פתוחות לכלל הציבור)
3. קופות גמל ותיקות (סגורות למצטרפים חדשים)

מדובר במגזר בו קיימים באופן אינהרנטי נתונים רגישים - מאגרי מידע הכוללים מידע אישי רגיש אודות עמיתים (כולל מידע רפואי, צוואות, ירושות וכו').

הנתונים במאגרי המידע חשופים לגורמים רבים (גוף מנהל, גוף מתפעל, מוקדי שירות לקוחות, סוכנים וכו')

התהליך שבוצע במספרים

51 שאלונים שהופצו

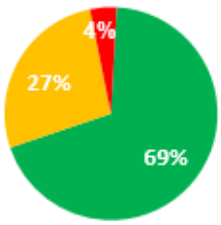
48 גופים שהשתתפו בפועל בהליך הפיקוח (ללא גופים שהוסרו מההליך או לא שיתפו פעולה)

25 דרישות להשלמת מידע חסר בכתב

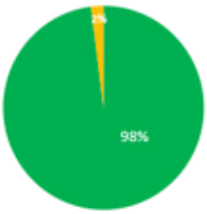
48 הנחיות לתיקון ליקויים

ממצאים – ליקויים מרכזיים:

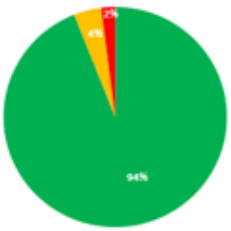
ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת הגופים המפוקחים במגזר



בקרה ארגונית



אבטחת מידע



ניהול מאגרי מידע

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

- מיקור חוץ - בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של ספק במיקור חוץ, בהתאם להוראות התקנות.
- מיקור חוץ – יש לוודא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע באופן עתי, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.
- יש לנסח הודעה לכל פניה בדיוור ישיר אשר תכיל את הנושאים הנדרשים בחוק.

- 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.
- יש לערוך ביקורות בנושא אבטחת מידע/הגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.

עיקר ההנחיות לתיקון ליקויים



- יש להבטיח כי המערכות יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה, על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות מאתרים שבהם מצויות המערכות, ושל כל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.
- תיעוד 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.
- הגבלת או מניעת אפשרות לחיבור התקנים ניידים, ושימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.
- 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.
- במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה מידי 18 חודשים, ולקיים דיון בממצאיהם תוך בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.

2. קופות גמל וקרנות השתלמות- תמונת מצב

2.1 כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2019 למאי 2020 במגזר קופות גמל וקרנות השתלמות.

2.2 רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר קופות גמל וקרנות ההשתלמות כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:

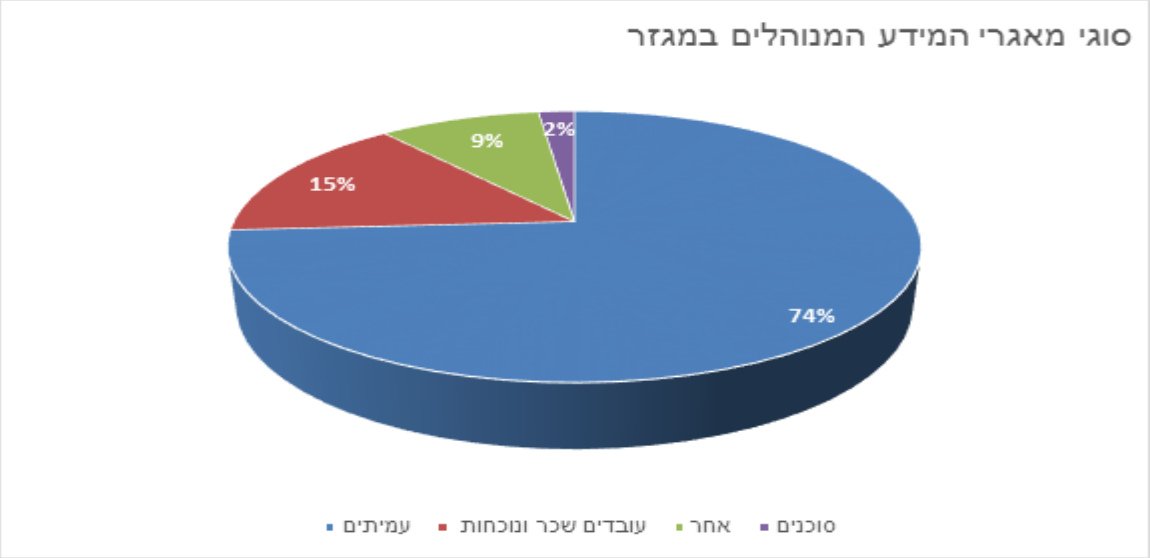
במגזר זה, באופן אינהרנטי נוכח אופי הפעילות, נשמר מידע אישי רגיש אודות עמיתים, עמיתים פוטנציאליים וכן עמיתים שחלו או נפטרו. רגישות המידע הקיים דורשת הקפדה מיוחדת על אבטחת המידע וכן שקיפות מלאה מול העמיתים או באי כוחם.

מדובר במגזר בו קיימים נתונים רגישים במאגרי מידע הכוללים מידע אישי רגיש אודות עמיתים (כולל מידע רפואי, צוואות, ירושות וכו').

הנתונים במאגרי המידע חשופים לגורמים רבים (גוף מנהל, גוף מתפעל, מוקדי שירות לקוחות, סוכנים וכו')

במגזר קיימים שלושה סוגי תאגידים עיקריים:

השתלמות ענפיות/ מפעליות/ סקטוריאליות (למגזים מסוימים, עובדי סקטור או מפעל מסוים)	קופות גמל וקרנות (פתוחות לכל הציבור)	קופות גמל ותיקות (סגורות למצטרפים חדשים)



2.3. תהליך עבודה

במטרה לפעול באופן המיטבי למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות נוקטת בגישה מבוססת סיכון, הבוחנת תדיר את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש לפעולותיה על המשק. הרשות פועלת על פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל המשק. על מנת לעמוד במכלול האתגרים העומדים לפתחה, פועלת הרשות על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, במגזרים שונים הכוללים מספר רב של נושאי מידע ומידע רגיש, וליישם את ממצאי הפעילות בצורה רוחבית.

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 האכיפה של הרשות. התוכנית נבנית בהתחשב בגורמים הבוחנים את כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר/נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

הליך הפיקוח החל ב- 51 גופים המשתייכים למגזר פיקוח קופות גמל וקרנות השתלמות, שנבחרו על ידי הרשות. בסופו של יום, בניכוי גופים אשר פעילותם מוזגה וגופים אשר הצהירו כי אינם מחזיקים מאגר מידע, השיבו 48 גופים לשאלוני הפיקוח.

בסיום ההליך, בכל 48 הגופים המפוקחים נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר יישומה. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

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 בדרישה למילוי שאלוני ביקורת, על בסיס קריטריונים שונים ובהם: [1]



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:

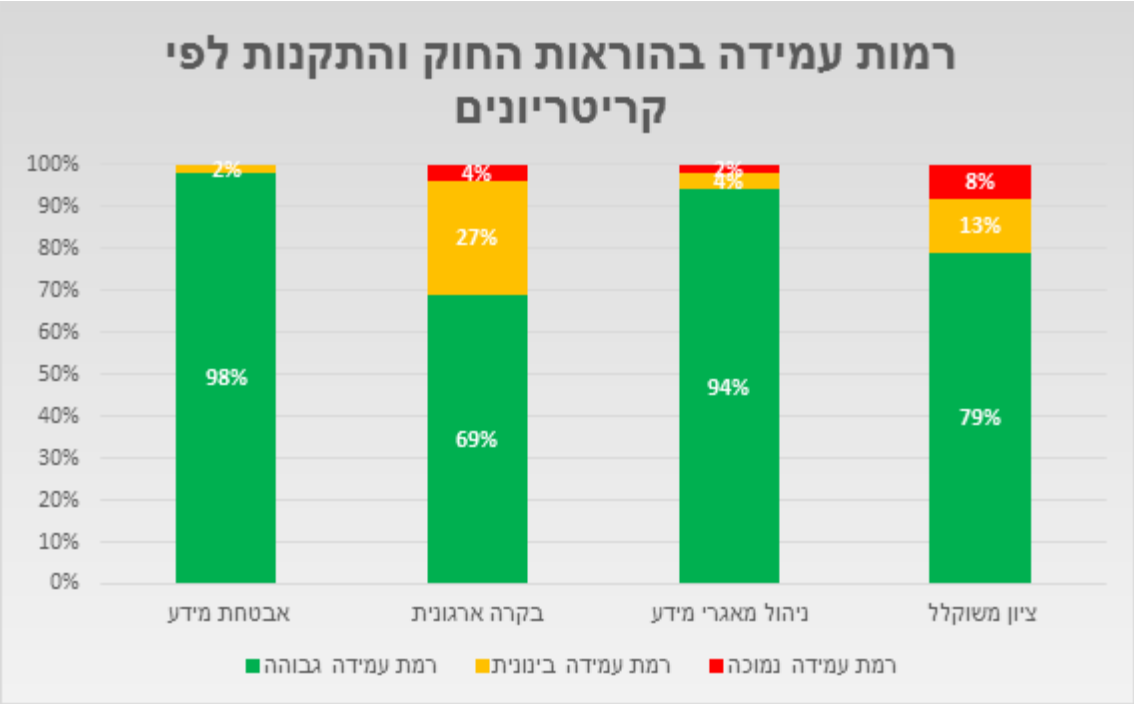
עמידה של בין 80%-100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;

[1] קריטריון עיבוד מידע אישי במיקור חוץ נבחן בהליך זה כקריטריון משנה תחת ניהול מאגרי מידע

עמידה של בין 50%-80% מוגדרת כרמת עמידה בינונית או חלקית;

עמידה של מתחת ל- 50% מוגדרת כרמת עמידה נמוכה.

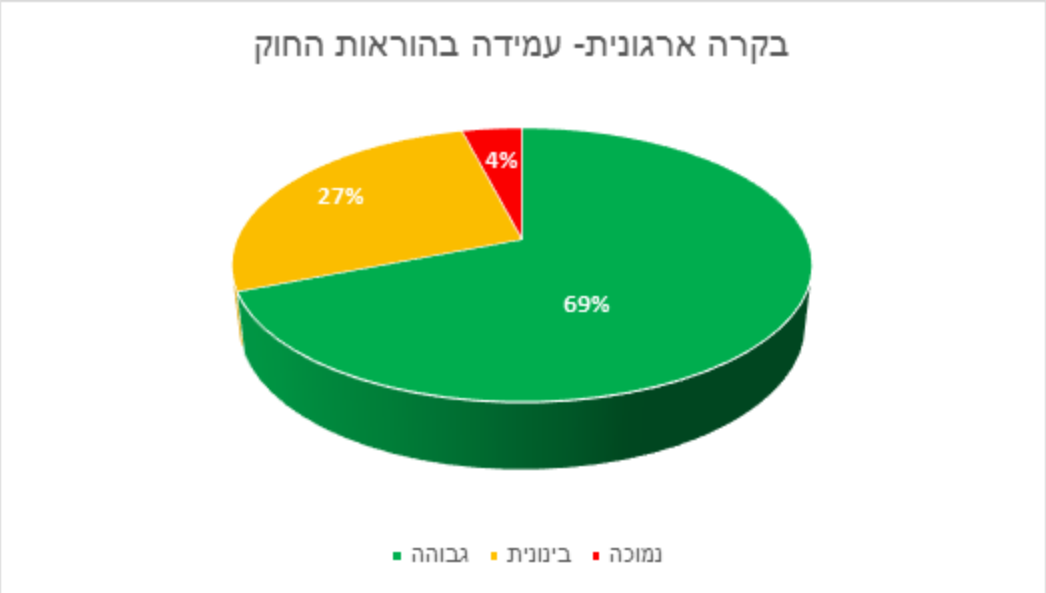
3. ממצאים והמלצות:

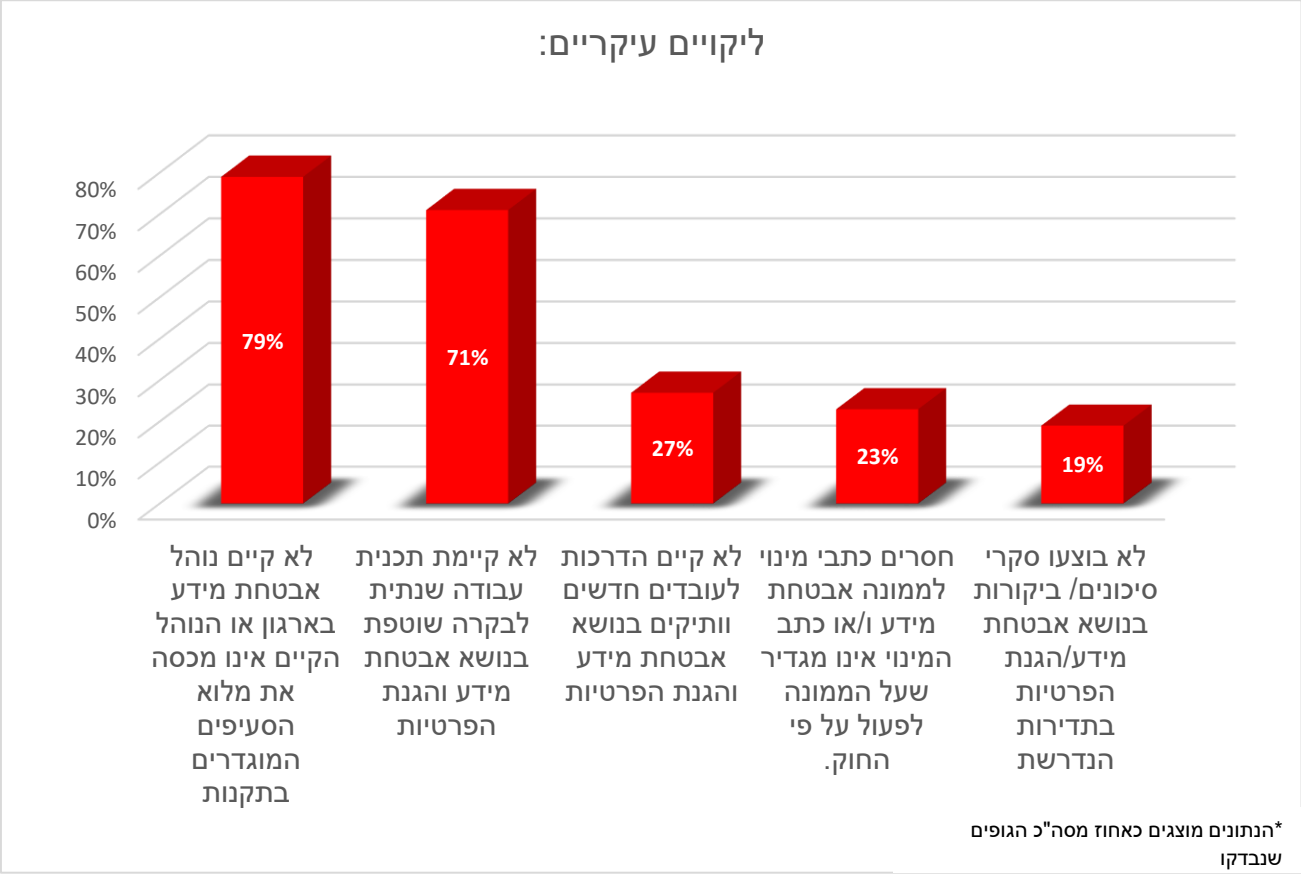


כעולה מהטבלה לעיל, בתחומי אבטחת מידע וניהול מאגרי המידע, רמת העמדה בתקנות הייתה גבוהה מאוד ועמדה על 98% ו- 94% בהתאמה. לעומתם, בתחומי הבקרה הארגונית והממשל התאגידי, רמת העמידה בתקנות הייתה בינונית ועמדה על 69%, עם 27% מהגופים במצב של עמידה חלקית ו- 4% במצב של עמידה חסרה כליל. בתחום העברת המידע בין גופים ציבוריים, רמת העמידה בתקנות הייתה נמוכה מאוד ועמדה על 29% במצב של עמידה חלקית בלבד בתקנות, ו- 71% במצב של עמידה חסרה.

3.1. בקרה ארגונית

ממצאים:





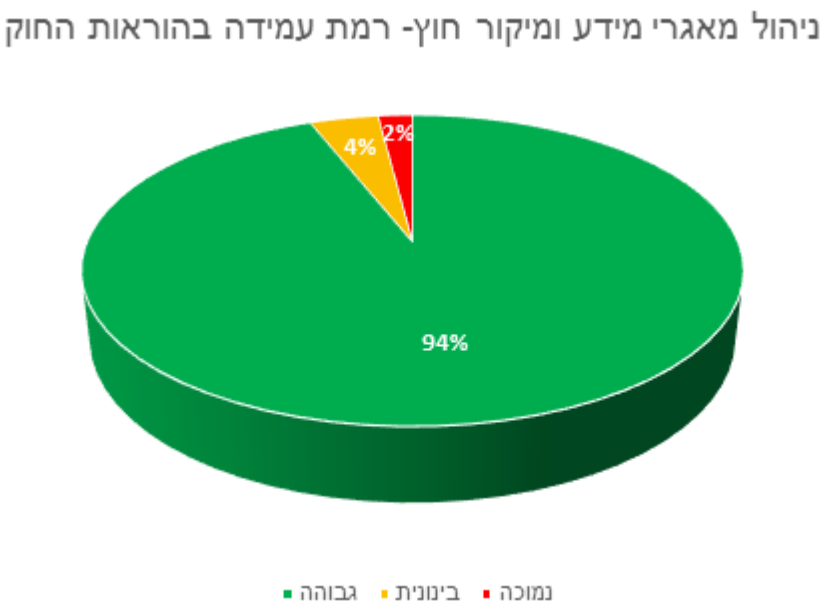
*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

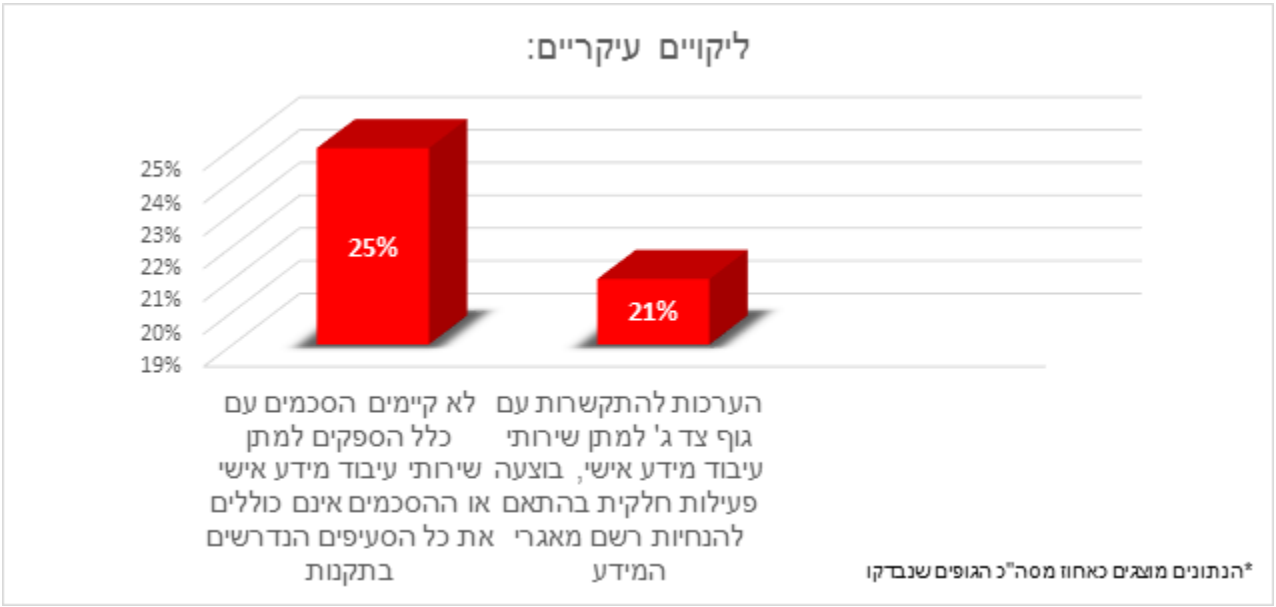
המלצות:

- כחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, תוך התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתבי מינוי רשמיים למנהל המאגר ולממונה אבטחת המידע היכן שמינויו נדרש, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, על הארגונים לגבש נוהל אבטחת מידע ולבחון את הצורך לעדכנו אחת לשנה, כנדרש בתקנות (תקנה 4).
- בהתאם להוראות התקנות, יש לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם מתן גישה למאגר המידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה זו לפחות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. יש לשמור את תיעוד החומרים שהועברו ואת התיעוד לביצוע ההדרכות.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או אחרים בעלי הרשאת גישה למאגר המידע, על מנת לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגרים. זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

3.2. ניהול מאגרי מידע ומיקור חוץ

ממצאים:



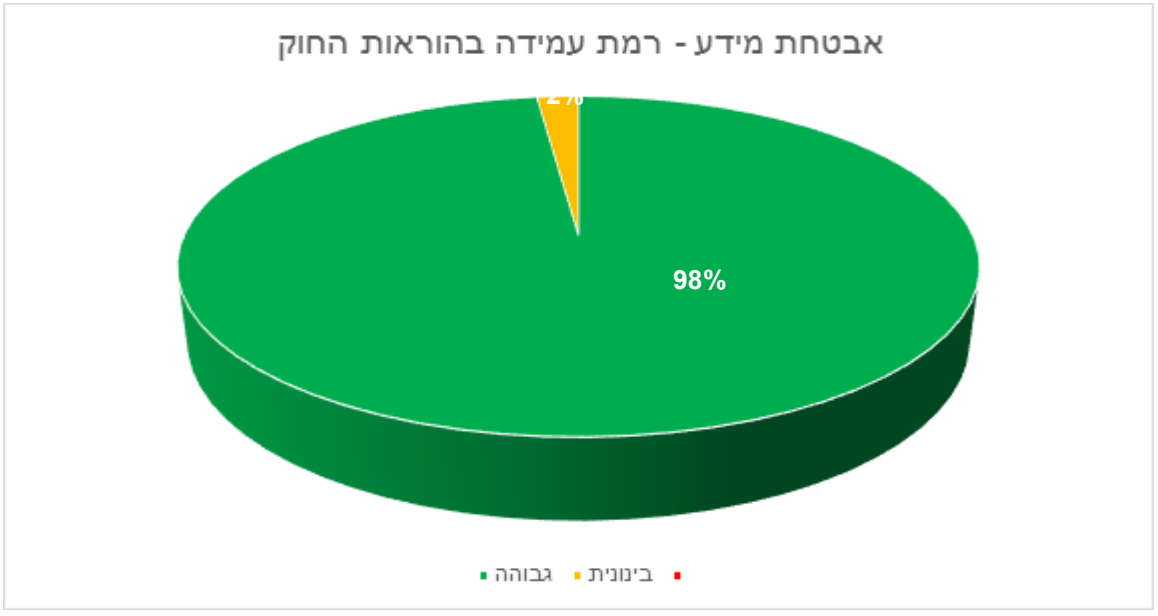


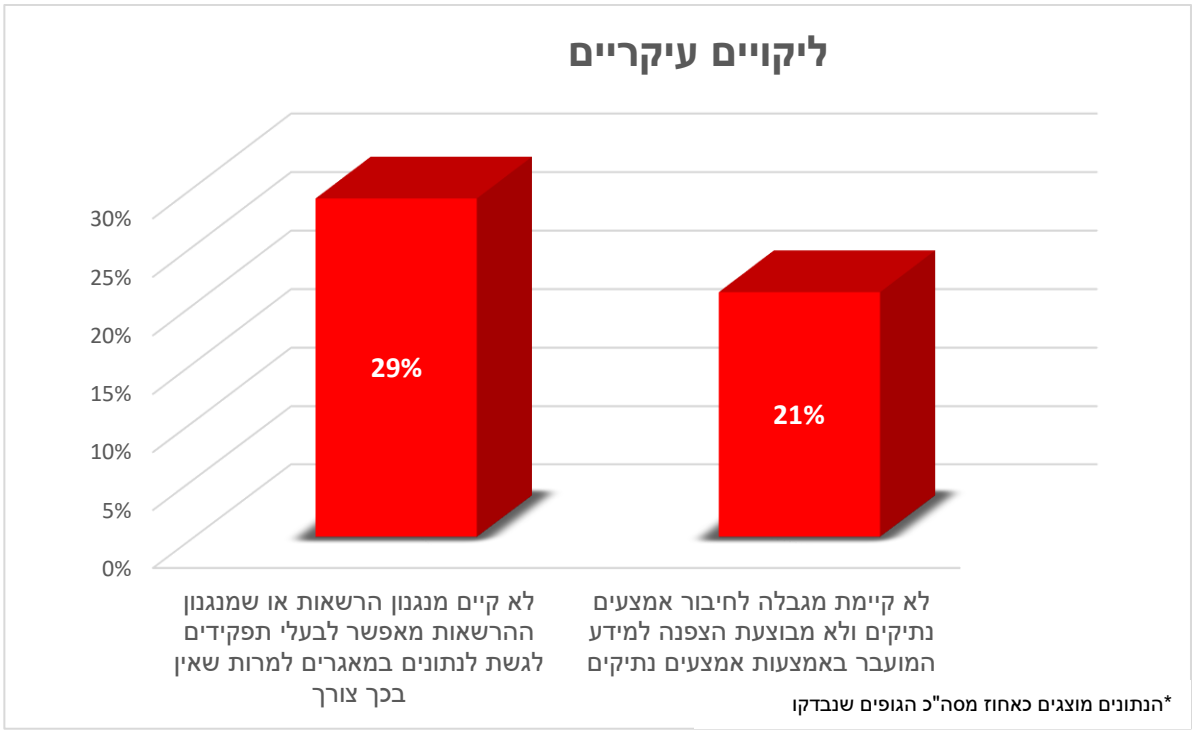
המלצות:

- יש ליידע את נושא המידע בדבר מקור הסמכות לאיסוף המידע על אודותיו. אם לא קיים מקור סמכות בחוק, יש לקבל את הסכמתו עבור איסוף המידע ושמירת פרטיו במאגרי המידע. זאת, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה עליו חובה חוקית למסור את המידע כאמור, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה, בהתאם להוראת סעיף 11 לחוק.
- בהתאם לתקנה 15 לתקנות אבטחת מידע, על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הרכיבים המנויים בתקנה 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.
- בעניין זה יש לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2/2011.

3.3. אבטחת מידע

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת לתקנות. בעניין זה על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשים במידע הנ"ל. עמדת הרשות היא כי רמת האבטחה של מאגרי המידע לעניין התקנות אינה מושפעת מכך שמאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הינו סך כל בעלי ההרשאה לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.
- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות. בנוסף, נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע .במאגרי מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמת אבטחה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.
- על הגופים לבחון את הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – מוצע להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על

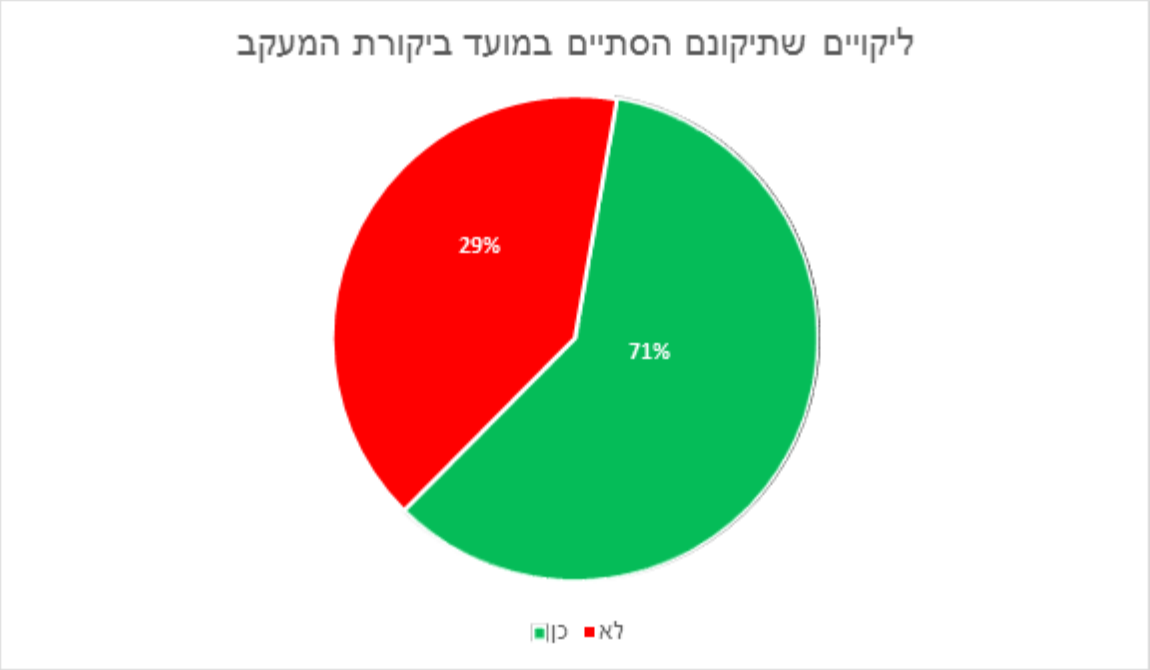
המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד למערכת, ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.

- על הגופים לוודא שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(2) לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה, הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 6 חודשים. כמו כן יש לעגן את מדיניות הסיסמאות בנוהל עבודה כנדרש בתקנה 9 (ב) לתקנות.
- על הארגון לנהל מנגנון תיעוד אוטומטי, שיאפשר ביקורת על הגישה למערכות המאגר ויכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה, כנדרש בתקנה 10. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
- בנוסף, על בעל מאגר המידע לקבוע נוהל בדיקה שגרתי עבור נתוני התיעוד של מנגנון הבקרה.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, לקביעת נהלים ולביצוע גיבויים ללוג נתוני האבטחה במאגר, באופן שיבטיח כי ניתן יהיה לשחזר בכל עת את הנתונים האמורים למצבם המקורי, כנדרש בתקנה 17 ותקנה 18 לתקנות.
- בהתאם לתקנה 2(ג) לתקנות אבטחת מידע, על הגופים לערוך, לפחות אחת לשנה, בחינה האם קיים במאגר מידע עודף, רב מן הנדרש למטרות המאגר, ולתעד בחינה זו.

4. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2020, נערך מעקב תיקון ליקויים במגזר קופות גמל וקרנות השתלמות, שבמסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, תוך מתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בנוסף, בוצעו על ידי הרשות להגנת הפרטיות, באופן מדגמי, פיקוחי מעקב על חלק מהגופים בהם נמצאו ליקויים, בין היתר תוך שקלול כמות הליקויים, סוג הליקוי והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישות הרשות לתיקון הליקויים. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים ואת העמידה בלוחות הזמנים שהגדירו ליישום התוכנית ותיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 98% מהגופים במגזר קופות גמל וקרנות השתלמות שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 71% מהליקויים יושמו וטופלו.



לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע לביצוע הליכי אכיפה משלימים, לרבות בכל הנוגע לבחינת תכניות העבודה לתיקון הליקויים וליישומן.

פיקוחי המעקב שבוצעו במגזר קופות גמל וקרנות השתלמות מעידים באופן חד משמעי על כך שעצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרוחב.

5. סיכום

כפי שעולה מהדוח, במגזר קופות גמל וקרן השתלמות, מנוהלים, באופן אינהרנטי, נתונים רגישים אודות עמיתים. נוכחנו כי מידת הטמעת התקנות במגזר זה הינה באופן כללי משביעת רצון. הנ"ל נובע בעיקר מהיותם גופים מוסדיים אשר כפופים לרגולציה של רשות שוק ההון ביטוח וחסכון.

במסגרת הליך הפיקוח נמצאה חולשה מסוימת בתחום הבקרה הארגונית ובכללה, היעדר הוצאת כתב מינוי רשמי לממונה אבטחת מידע, אי עיגון כלל נהלי העבודה כנדרש, ותוכנית עבודה שנתית בנושא אבטחת מידע והגנת הפרטיות ברמה נמוכה. מצאנו כי עובדים אינם עוברים הדרכות בתדירות הנדרשת, וכי לא בוצעו סקרי סיכונים או ביקורות בנושא אבטחת מידע/הגנת הפרטיות בתדירות הנדרשת.

כמו כן, ארגונים אינם מודעים לכך שהינם מוגדרים כגופים ציבוריים בהתאם לצו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו-1986 ולאור זאת לא פועלים בהתאם לחובות הנדרשות מהם, לרבות מינוי ועדה להעברת מידע בין גופים ציבוריים ומתן הודעה לרשות בדבר קבלת מידע דרך קבע מגופים ציבוריים אחרים (סעיף 23ד(ג) לחוק).

בהיבטי אבטחת המידע שנדרשים מטעם הארגון, זוהתה חולשה רוחבית בנושאים מסוימים, דוגמת שימוש באמצעים נתיקים וניהול לוקה בחסר של מנגנון ההרשאות.

בנוסף, בעת היערכות להתקשרות עם גוף צד ג' למתן שירותי עיבוד מידע אישי, ארגונים אינם פועלים בהתאם לתקנה 15 לתקנות אבטחת מידע, ולהנחיות רשם מאגרי המידע מס' 2/2011.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי מאגרי מידע והמחזיקים בהם 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 הזכות החוקתית לפרטיות.

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר קופות גמל וקרנות השתלמות, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.