



דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב עמותות ומגזר שלישי



שבט תשפ"ד
פברואר 2024



תוכן עניינים

1.תקציר	
מנהלים.....	3
1.1.מגזר עמותות ומגזר שלישי.....	3
1.2.תהליך העבודה.....	3
1.3.ליקויים, מסקנות והמלצות עיקריות.....	4
2.עמותות ומגזר שלישי - תמונת מצב.....	6
2.1.כללי.....	7
2.2.רקע על המגזר.....	7
2.3.תהליך עבודה.....	9
2.4.הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו.....	10
3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות:.....	11
3.1.בקרה ארגונית.....	12
3.2.ניהול מאגרי מידע ועיבוד מידע אישי במיקור חוץ.....	14
3.3.אבטחת מידע.....	16
3.4.העברת מידע בין הגופים הציבוריים.....	19
4.מסקנות - תמונת מצב.....	21
5.מעקב תיקון ליקויים.....	23
6.סיכום.....	24



1. תקציר מנהלים

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

1.1. מגזר עמותות ומגזר שלישי

הרשות להגנת הפרטיות הגדירה את מגזר עמותות ומגזר שלישי בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה בהיבטי הפרטיות, הבאים לידי ביטוי במספר היבטים:

1. איסוף, החזקה ושימוש במידע רגיש, ובכלל זה מידע סודי ומידע ובעל יסודות של צנעת הפרט, אודות אנשים אשר מסתייעים בעמותות השונות ונעזרים בשירותיהן.
2. מאגרי מידע גדולים מאוד במגוון רחב של עמותות עם אוכלוסיות מידע שונות.
3. מגוון רחב של עמותות גדולות וקטנות אשר בחלקן אין מחלקות ייעודיות לטיפול בנושא הגנת הפרטיות.

ניהול מאגרים, בהתייחס למאפייניו הייחודיים של המגזר, מחייב את אותם גופים לעמוד בדרישות חוק הגנת הפרטיות ותקנות אבטחת המידע, לקיים את חובת היידוע ולקיים בקרה ארגונית. נוכח כל אלה הרשות להגנת הפרטיות הגדירה מגזר זה כיעד פיקוח רוחב משמעותי.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב הרשות פנתה בדרישה למילוי שאלוני ביקורת ל-33 גופים הפועלים במסגרת של עמותות ומגזר שלישי.

שאלוני הביקורת בחנו ארבעה קריטריונים בתחום הגנת הפרטיות:

(1) בקרה ארגונית (2) ניהול מאגרי מידע (3) אבטחת מידע (4) העברת מידע בין גופים ציבוריים בגופים הרלוונטיים.

הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו.



1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר עמותות ומגזר שלישי נמצאה רמת עמידה בינונית-נמוכה בכל הקשור בניהול מאגרי מידע ובבקרה ארגונית, לעניין העברת מידע בין גופים ציבוריים, נמצאה רמת עמידה נמוכה, ובקריטריון אבטחת מידע נמצא כי שליש מכלל הגופים אינם עומדים או שעומדים ברמה חלקית בדרישות החוק והתקנות.

לאור הממצאים שעלו מהליך פיקוח הרוחב, קיבלו כל 24 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם וכן דו"ח הנחיות לכלל הגופים הפועלים במגזר זה המפרט את הצעדים שעליהם לנקוט בכדי לעמוד בדרישות החוק והתקנות.



ממצאי הליך פיקוח רחב בקרב מגזר עמותות ומגזר שלישי

דו"ח פיקוח רחב 2021-2022



תוכן המאגר – מידע רגיש
ובכלל זה מידע רגיש אודות
אנשים אשר מסתייעים
בעמותות השונות ונעזרים
בשירותיהן.

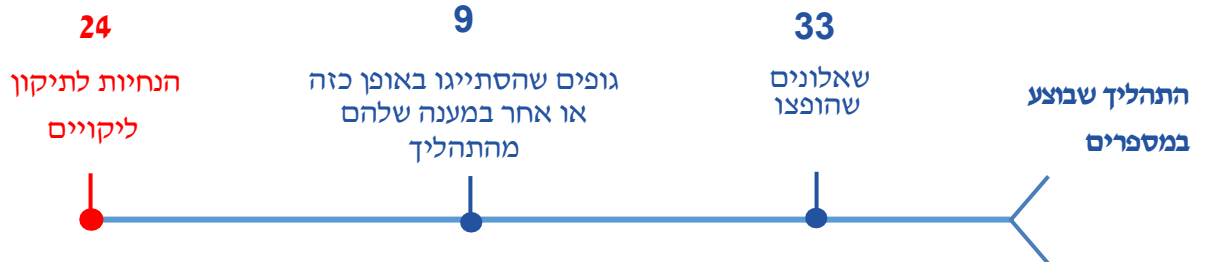


מאגרי מידע גדולים מאוד
במגוון רחב של עמותות
העוסקות בעיקרן במתן סיוע
לאוכלוסיות מוחלשות.
מגוון רחב של עמותות גדולות
וקטנות אשר בחלקן אין
מחלקות ייעודיות לטיפול
בנושא הגנת פרטיות



תקופת הפיקוח - תקופת
הקורונה יצרה עומס פניות של
נתמכים כמעט בכל עמותה
לנוכח המשבר החברתי-כלכלי.
כפועל יוצא מכך נאסף מידע
רב אודות נתמכים וגדלה כמות
הרשומות במאגרי העמותות

אתגרים ומאפיינים
ייחודיים של מגזר
עמותות ומגזר שלישי





- מיקור 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 עימו הם התקשרו לצורך קבלת שירות הכרוך במתן גישה למאגר, כאשר יש לקבוע במפורש בהסכם את כל הוראות תקנה 15(א)(2) לתקנות הגנת הפרטיות (אבטחת מידע).**
- מיקור חוץ - יש לוודא כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם ולהוראות ההסכמה עימו והוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.**
- על כל פניה בדיוור ישיר להכיל את הפרטים הנדרשים לפי הוראות החוק.**
- בגוף המחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8, יש למנות ממנה 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.**
- עריכת ביקורות בנושא אבטחת מידע מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.**

עיקר ההנחיות לתיקון ליקויים



- יש להבטיח כי מערכות המאגר 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 מערכות תשתיות, חומרה, סוגי רכיבי תקשורת ואבטחת מידע, ושל כל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.**
- יש לבצע תיעוד של כל אירוע המעלה חשש לאירוע אבטחה. בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע.**
- יש לבחון את הצורך בחיבור התקנים ניידים ולפעול להגבלת או מניעת אפשרות לחיבור התקנים ניידים. במקרים בהם יוגדר כי קיים צורך בשימוש בהתקנים ניידים, יש להצפין את הנתונים באמצעות שימוש 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 אחת לשנה וחצי, ולקיים דיון בממצאיהם תוך בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ולפעול לתיקון הליקויים שהתגלו במסגרת המבדקים.**



2. עמותות ומגזר שלישי - תמונת מצב

2.1 כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בין השנים 2021-2022 במגזר עמותות ומגזר שלישי.

2.2 רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר עמותות ומגזר שלישי כיעד פיקוח רחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:
מידע רגיש, אודות אנשים אשר מסתייעים בעמותות השונות ונעזרים בשירותיהן.
כמו-כן, מאגרי מידע גדולים מאוד במגוון רחב של עמותות עם אוכלוסיות מידע שונות. בנוסף, ישנו מגוון רחב של עמותות גדולות וקטנות אשר בחלקן אין מודעות לחשיבות בטיפול בנושא הגנת הפרטיות.
להלן התובנות המרכזיות בנוגע ליעד פיקוח הרוחב:

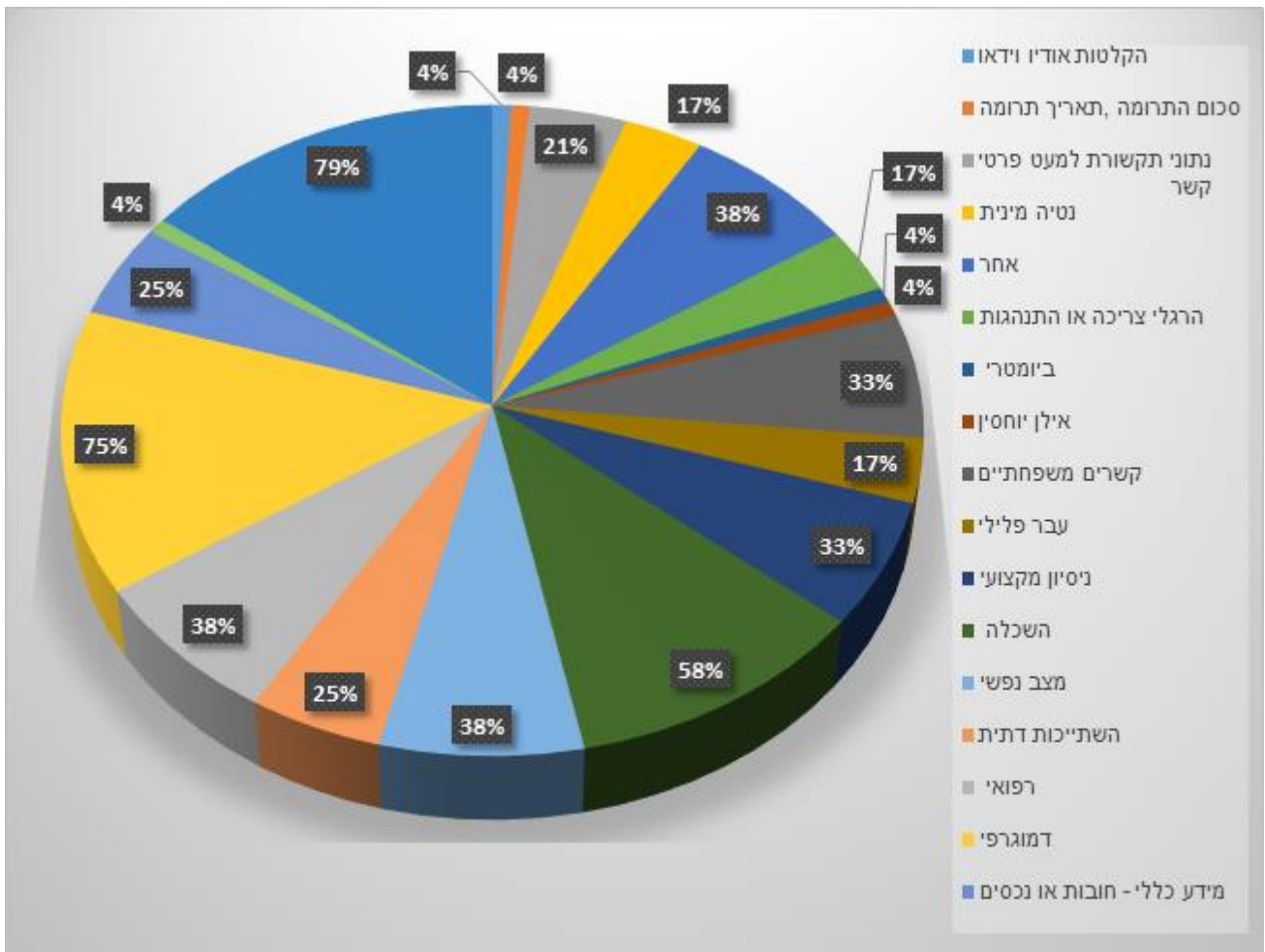
מבנה הארגון

מגוון רחב של עמותות גדולות וקטנות אשר בחלקן אין מודעות מספקת לטיפול בנושא הגנת הפרטיות.

תקופת הפיקוח

תקופת הקורונה מהווה תקופה מאתגרת מאוד שכן מגזר זה היה פעיל באופן רציף ואף מוגבר, ולמרות המגבלות הקשורות בתקופה - נדרש לצלוח אותה תוך הפגנת רציפות תפקודית.

התפלגות מאגרי המידע במגזר:



*הנתונים מוצגים כאחוז מסך כל הגופים שנבדקו

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

הליך הפיקוח בוצע ב-24 גופים מפקחים, במגזר עמותות ומגזר שלישי, שנבחרו על ידי הרשות במהלך התהליך. בסיום ההליך נמצאו בכולם ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את אותם גופים מפקחים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים, וממצאי 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 מכוח

במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת, הבוחנים זאת על בסיס קריטריונים שונים ובהם:



רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הגופים, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:

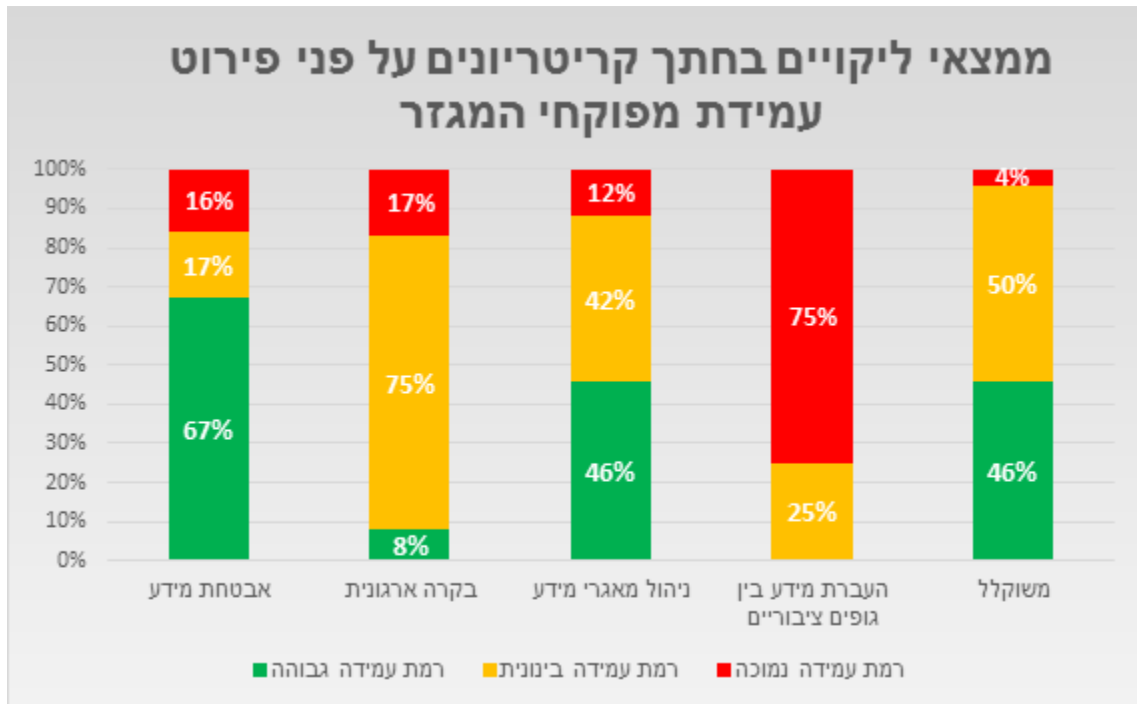
עמידה של בין 80%-100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;

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

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



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



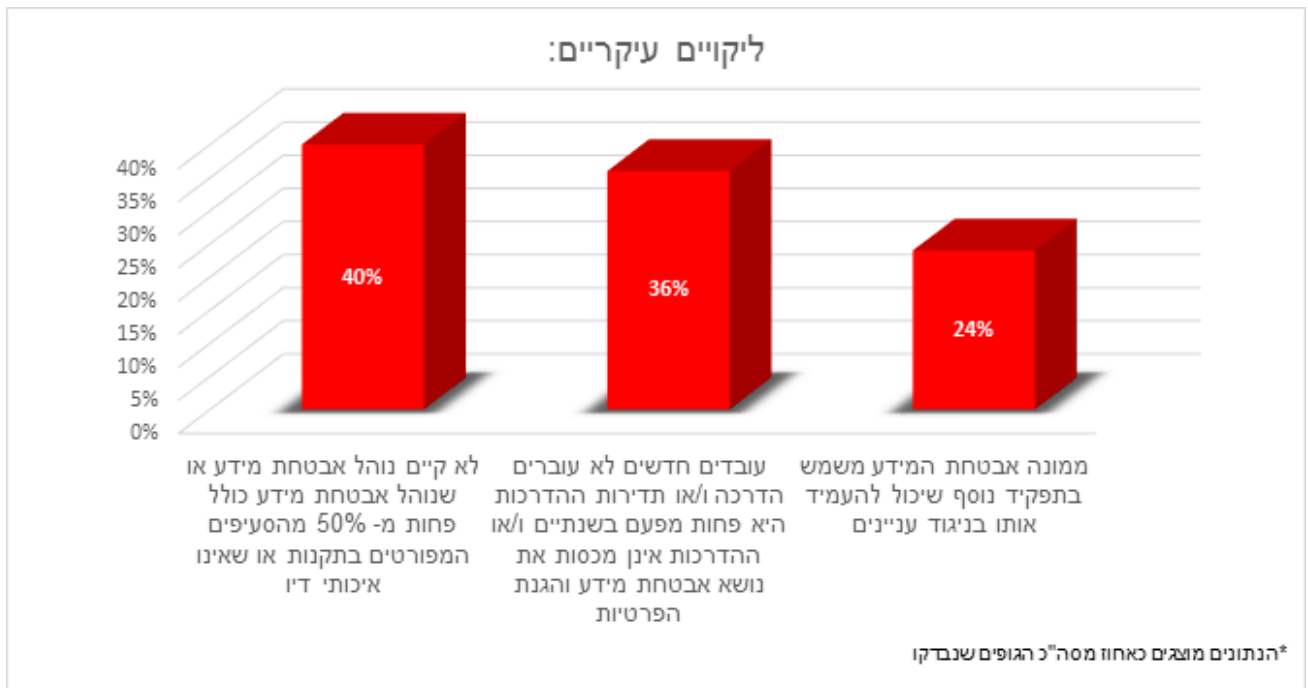
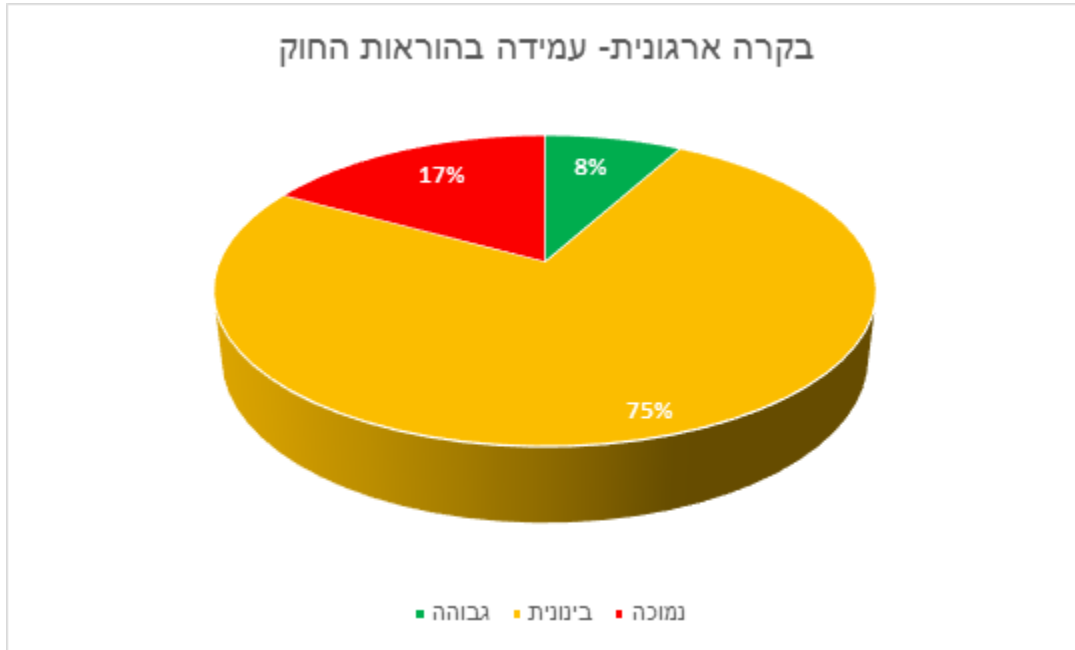
בתחום אבטחת מידע כ-17% מן הגופים לא עומדים בדרישות החוק באופן מלא, וכ-16% מן הגופים מצויים ברמת עמידה נמוכה.

בתחום ניהול מאגרי מידע, כ-42% מן הגופים נמצאים ברמת עמידה בינונית ו-12% מהגופים ברמת עמידה נמוכה.

בציון המשוקלל, כ-50% מן הגופים הציגו רמת עמידה חלקית בלבד בשקלול כל התחומים שנבדקו, מתוכם כ-4% מהגופים מצויים ברמת עמידה נמוכה.

3.1 בקרה ארגונית

ממצאים:

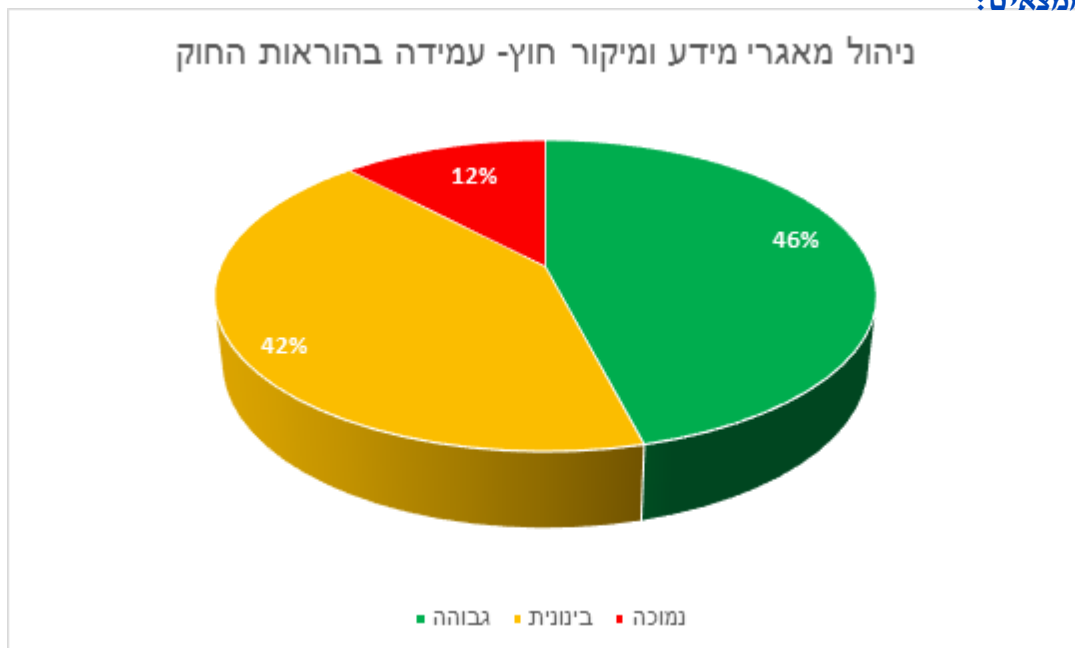


המלצות:

- כחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבעלותם 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 ולמונה 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 יקבלו 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 וכן התיעוד לביצוע ההדרכות.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או בעלי הרשאות גישה אחרים למאגר המידע, על מנת לברר שאין חשש כי בעל הרשאה אינו מתאים לקבלת גישה למידע המצוי במאגרים. זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

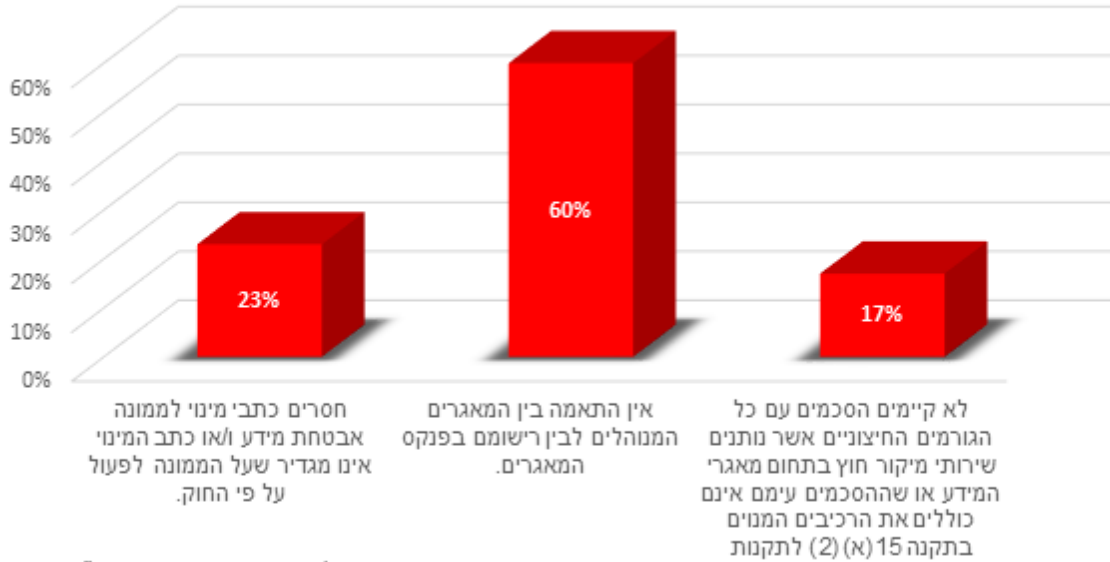
3.2. ניהול מאגרי מידע ומיקור חוץ

ממצאים:





ליקויים עיקריים:



*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

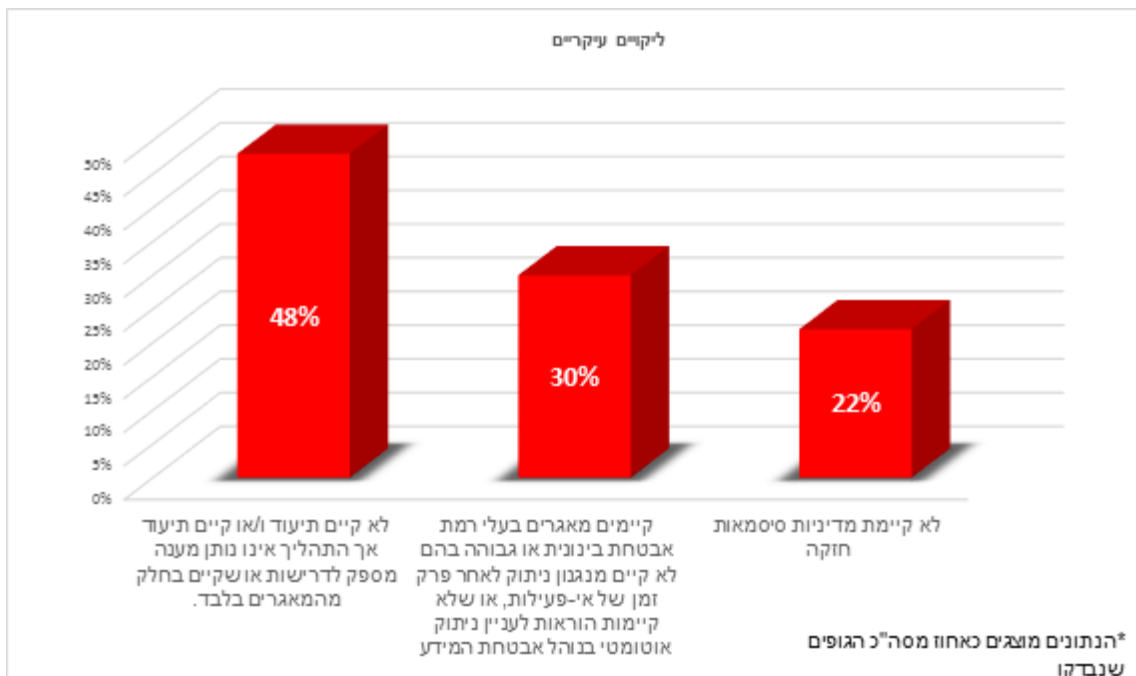
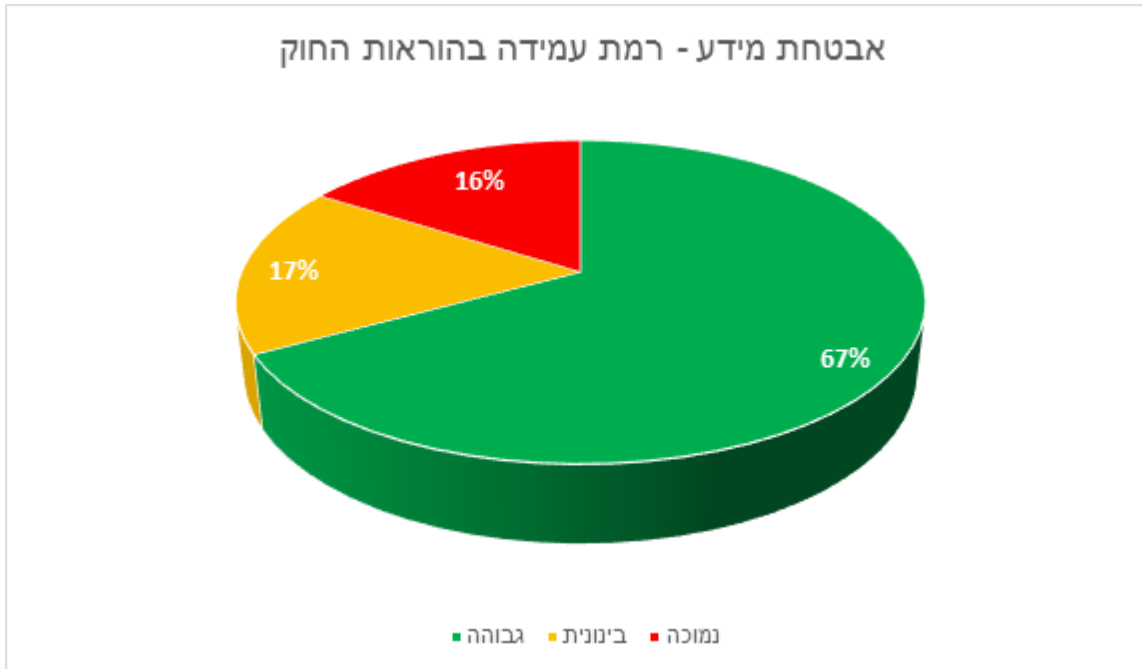
המלצות:

- מגזר עמותות ומגזר שלישי אוסף מידע רגיש הנוגע להתנהלות יום יומית של משתמשים, לרוב מאוכלוסיות מוחלשות. לנוכח המידע הרגיש והעובדה שמדובר על מגזר עמותות ומגזר שלישי במהותו, ישנו משקל רב לעובדה שבתחום אבטחת מידע כ- 33% מן הגופים מצויים ברמת עמידה בינונית ונמוכה, ולכן נדרשת הגברת המודעות להפעלת המנגנונים שנבנו במסגרת הבקרה הארגונית באופן מלא ויעיל על מנת שיבטיחו עמידה מלאה בדרישות תקנות אבטחת המידע. זאת ועוד, בשל השימוש הנרחב של הגופים באיסוף מידע ועבודה מול אנשים המשתמשים בשירותיהם, יש להקפיד הקפדה יתרה על אבטחת המידע ושמירה על פרטיות המשתמשים.
- בתחום ניהול מאגרי מידע כשליש מן הגופים מצויים, כאמור, ברמת עמידה בינונית בלבד. הגורם המרכזי לליקויים בתחום זה הינו עמידה חלקית בדרישות התקנות והנחיות הרשם בהתקשרות עם גורם חיצוני לצורך עיבוד או ניהול מידע המהווה סיכון משמעותית למידע של הארגון.¹ נדרשת הגברת המודעות בקרב מגזר עמותות ומגזר שלישי לעמידה מלאה בכלל הדרישות הנוגעות לאבטחת המידע, תוך הבנת החשיבות להגנה על מידע רגיש, הנאסף בהיקפים גדולים ותוך שימוש משמעותי באמצעי ניהול ועיבוד מידע דיגיטליים. כן, נדרשת תשומת לב מיוחדת להגברת המודעות במגזר לדרישות החוק במתן גישה לגורם חיצוני לצורך עיבוד או ניהול מידע של הארגון.

¹ לקריאה נוספת ר' מדריך פעולה ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) בעת התקשרות עם גורם חיצוני

3.3. אבטחת מידע

ממצאים:



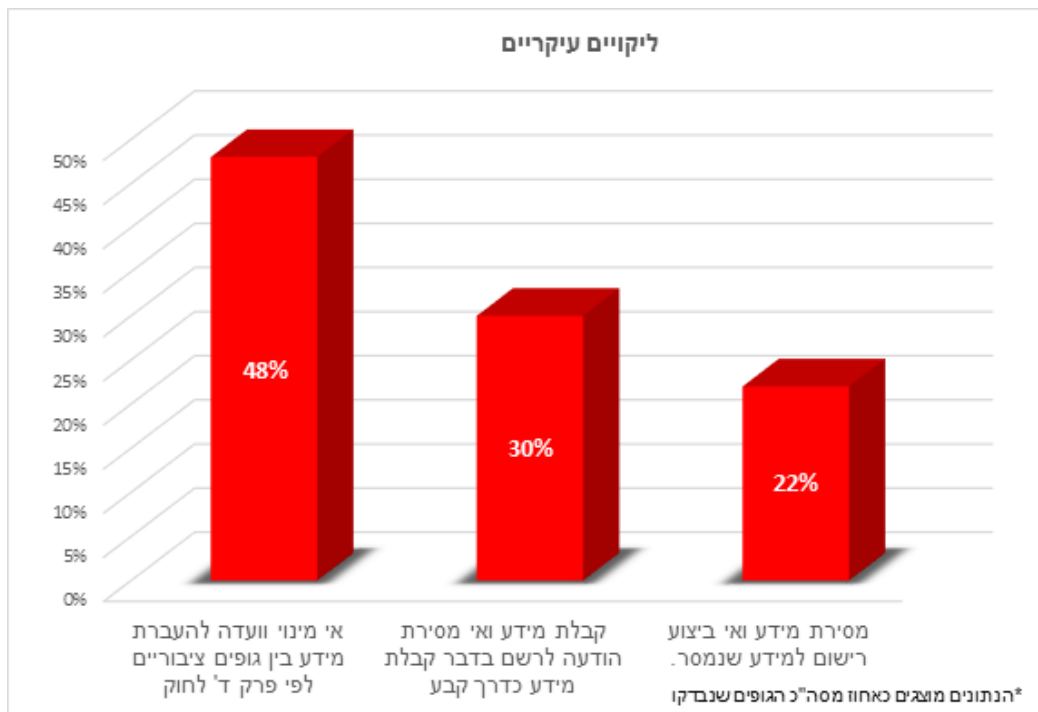
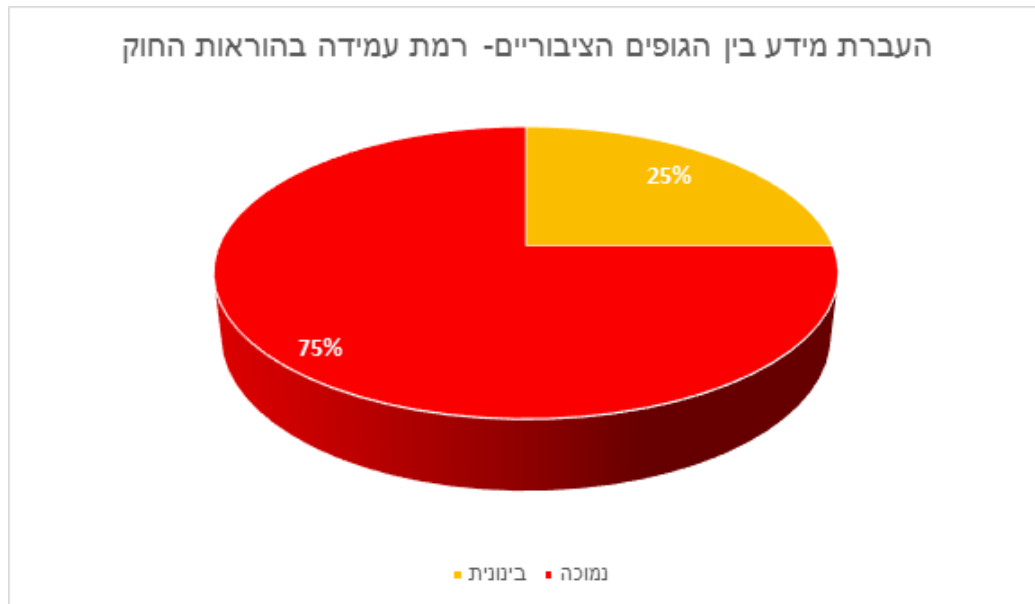


המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת בתקנות, בדרך של בדיקת סוג המידע שהם אוספים, והמטרות והשימושים שנעשים במידע הנ"ל.
- בתחום אבטחת מידע נמצאו במצטבר סוגי ליקויים בנושאים בעלי חשיבות רבה. בחלק מן הגופים נמצאו ליקויים כגון היעדר מדיניות סיסמאות חזקה, אי קיום מבדקי חדירה וסקרי סיכונים בתדירות הנדרשת, תיעוד גישה חלקי ועוד.
- 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, ולקביעת נהלים וביצוע 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. בין היתר, יש לבחון האם מצוי במאגר מידע עודף בנוגע לדיירים שעזבו או שנפטרו, ששוב אינו נדרש עוד למטרות המאגר.

3.4. העברת מידע בין הגופים הציבוריים²



² קטגוריה זאת רלוונטית רק לגופים אשר דיווחו כי הם גוף ציבורי, בהתאם לסעיף 23 לחוק הגנת הפרטיות.



המלצות:

- גופים המהווים גוף ציבורי, כהגדרתו בסעיף 23 לחוק הגנת הפרטיות, נדרשים לוודא כי הוקמה ועדה להעברת מידע בין גופים ציבוריים, והיא מתכנסת לצורך דיון בניהול מידע ואבטחתו. וזאת, בהתאם להוראות פרק ד' לחוק הגנת הפרטיות ותקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים, תשמ"ו-1986).
- גוף ציבורי המוסר מידע בהתאם לסעיף 23 לחוק הגנת הפרטיות יקיים רישום של המידע שנמסר.
- גוף ציבורי המקבל דרך קבע מידע בהתאם לסעיף 23 לחוק הגנת הפרטיות, והמידע נאגר במאגר מידע, יודיע על כך לרשם ועובדה זו תיכלל בפרטי רשימת מאגרי המידע לפי סעיף 12.

4. מסקנות - תמונת מצב

להלן התובנות המרכזיות בנוגע ליעד פיקוח הרוחב:

4.1. אבטחת מידע

- יש להגדיר ניתוק אוטומטי של מאגרי המידע בעלי רמת אבטחת בינונית ומעלה לאחר פרק זמן סביר של אי פעילות במערכת.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, נדרשים הגופים לקבוע בנוהל אבטחת המידע את אופן הגישה למאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה.
- על הגופים המפוקחים לבצע תיעוד של כל אירוע המעלה חשש לאירועי אבטחה. התיעוד יבוסס ככל האפשר על רישום אוטומטי.
- נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, יגדיר את מנגנוני הדיווח ואופן הדיווח ויכלול בתוכו תהליך של הפקת לקחים עבור אירועים שהתרחשו.

4.2. ניהול מאגרי מידע

- הגופים המפוקחים נדרשים למנות מנהל מאגר מידע בהתאם לאמור בחוק ובתקנות.
- על המפוקחים לוודא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע, בהתאם לתקנה 15, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.

4.3. בקרה ארגונית וממשל תאגידי

- הגופים המפוקחים נדרשים, בין היתר, לוודא כי ממונה אבטחת המידע אינו משמש בתפקיד נוסף שיכול להעמיד אותו בניגוד עניינים.



- על הגופים לגבש נוהל אבטחת מידע אשר יכלול בין היתר התייחסות לנושאי אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'.
- על הגופים המפוקחים לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם יקבלו גישה למאגר המידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה זו לפחות אחת לשנתיים.

4.4. העברת מידע בין גופים ציבוריים

- עבור גופים שנדרשו לעמוד בקריטריון זה, בשל היותם "גוף ציבורי" כהגדרתו בסעיף 23 לחוק הגנת הפרטיות, עיקר הליקויים היו בנושאים של אי מינוי ועדה להעברת מידע בין גופים ציבוריים לפי פרק ד' לחוק, קבלת מידע ואי מסירת הודעה לרשם בדבר קבלת מידע כדרך קבע.

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2023, נערך מעקב תיקון ליקויים במגזר עמותות ומגזר שלישי, שבמסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בנוסף, בוצעה ע"י הרשות להגנת הפרטיות, באופן מדגמי, פיקוחי מעקב על חלק מהגופים בהם נמצאו ליקויים, בין היתר תוך שקלול מספר הליקויים, סוג הליקוי והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישות הרשות תיקון הליקויים. בעת פיקוח המעקב בוחנת 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 50% מהגופים במגזר עמותות ומגזר שלישי שקיבלו הנחיות לתיקון ליקויים, נמצא כי במועד הביקורת הגופים סיימו לתקן 18% מכלל הליקויים.

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

פיקוחי המעקב שבוצעו במגזר עמותות ומגזר שלישי מעידים באופן חד משמעי על כך שעצם קיום הליכי פיקוח הרחב 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 הרחב.



6. סיכום

כאמור, קיימים סיכונים לא מעטים לפרטיות האנשים המסתייעים בשירותי עמותות ומגזר שלישי, אשר נובעים מכך שגופים אלו מנהלים מידע רב, מזוהה ורגיש, הן בעצמם והן באמצעות גורמים חיצוניים שמעניקים להם שירותי מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות חוק הגנת הפרטיות ותקנות אבטחת מידע על מנת להגן על הזכות לפרטיות ואת חובות אבטחת המידע. ממצאי הליך פיקוח הרוחב במגזר עמותות ומגזר שלישי מצביעים על פערים בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע, בקרה ארגונית וממשל תאגידי, ניהול מאגרי מידע והעברת מידע בין גופים ציבוריים. 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 מפוקחים במגזר זה אשר הונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על זכות הציבור לפרטיות.

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