אדר ב'
תשפ"ב

מרץ
2021



דוח סיכום פיקוחי הרוחב שבוצעו על-ידי הרשות להגנת הפרטיות

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

תוכן

דוח סיכום פיקוחי הרוחב שבוצעו על ידי הרשות להגנת הפרטיות..... 2
רקע..... 2
פיקוח רוחב..... 2
סיכום של פעילות פיקוח לפי שנים..... 4
סיכום של פעילות פיקוח הרוחב במספרים..... 4
מספר גופים שנבדקו בקרב מגזרים בהם פורסמו דוחות מגזריים מתוך ממצאי הפיקוח..... 4
ממוצע רמות עמידה לפי קריטריונים..... 5
תהליך העבודה..... 5
מיפוי רמות סיכון..... 6
הקריטריונים הנבדקים ואופן קביעת רמת העמידה בהוראות החוק והתקנות מכוחו:..... 8
המגזרים שנבדקו, רקע, מאפיינים וסיכונים:..... 9
מגזר רשויות מקומיות..... 10
גופים המנהלים פלטפורמות לימודיות וחינוכיות לקטינים..... 11
מגזר חברות אחסון ועיבוד מאגרי מידע..... 11
מכונים רפואיים ומעבדות רפואיות..... 12
מגזר מרפאות בריאות הנפש..... 12
מגזר נותני שירות סיוע במימוש זכויות רפואיות..... 13
השוואת רמת העמידה בין המגזרים השונים שנבדקו ביחס לקריטריונים זהים..... 14
בקרה ארגונית - רמות עמידה לפי מגזר..... 14
ניהול מאגרי מידע - רמות עמידה לפי מגזר..... 15
אבטחת מידע - רמות עמידה לפי מגזר..... 17
עיבוד מידע אישי במיקור חוץ - רמות עמידה לפי מגזר..... 18
העברת מידע בין גופים ציבוריים - רמות עמידה לפי מגזר..... 20
פיקוחי מעקב..... 21
שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב לפי מגזרים..... 21
זיהוי ורישום מאגרים בעקבות פיקוח הרוחב..... 22
עדכון הסכמי עבודה מול מיקור חוץ בהתאם לתקנה 15 בעקבות פיקוח הרוחב..... 24
מינוי ממונה הגנת הפרטיות שדווחו בעת פיקוח הרוחב לשנים 2019-2020..... 24
סיכום..... 26

דוח סיכום פיקוחי הרוחב שבוצעו על ידי הרשות להגנת הפרטיות

רקע

הרשות להגנת הפרטיות (להלן "הרשות") הינה הגוף המאסדר, המפקח והאוכף על פי חוק הגנת הפרטיות בישראל. ברגולטור הפועל להגנה על זכות היסוד לפרטיות, הרשות להגנת הפרטיות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים ועל ביצורה של הזכות לפרטיות. לתכלית זו הרשות מפעילה רגולציה, לרבות אכיפה מנהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי.

דו"ח זה מסכם ומנתח את הממצאים שפורסמו לציבור מהליכי פיקוח רוחב שבוצעו ב-7 מגזרים שונים, מתוך 16 מגזרים שלמים שנבדקו מיום הקמת מערך פיקוח הרוחב בשנת 2018 ועד היום. דו"ח זה נועד להציג תובנות, מסקנות וממצאים בנוגע להליך פיקוח הרוחב בכלל ובנוגע לעמידה בחוק הגנת הפרטיות, התשמ"א-1981 (להלן – "החוק") ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - "התקנות"), כמו גם את החולשות והסיכונים בשמירה על מאגרים במגזרים מסוימים וההבדלים ביניהם, בהתאם לקריטריונים שונים שהוגדרו לבחינה כחלק מהליך סדור אותו מבצעת הרשות להגנת הפרטיות.

פיקוח רוחב

מערך פיקוח הרוחב הוקם בשנת 2018, לצד זרועות האכיפה הפלילית והמנהלית ברשות להגנת הפרטיות ובמסגרת סמכויותיה. המערך מקיים פיקוחי רוחב מגזריים או נושאיים לבחינת יישום החוק והתקנות במגזרים שונים במשק הישראלי. המערך פועל לאיתור הפרות של החוק, להגברת מודעות המשק להוראות החוק, לאיתור כשלים ענפיים הדורשים התערבות והנחיות מיוחדות ולקבלת תמונת מצב מגזרית לגבי עמידה בהוראות הדין.

הליך פיקוח הרוחב הינו הליך סדור בעל אבני דרך ויעדים הכוללים שלבים קבועים להגשמת הליך האכיפה מתחילתו עד סופו, החל במיפוי וקביעת המגזרים בעלי הסיכון לפרטיות אותם בכוונת הרשות לבחון בהתאם למדיניותה ובהתאם לסקרי סיכונים שנתיים אותם מבצעת הרשות, המשך בזיהוי הגופים המתאימים בכל מגזר על ידי קביעת קריטריונים מתאימים, ובלה בהפצת שאלוני פיקוח, הפקת דוחות ביניים, הפצת שאלוני השלמת ידיעות ומסמכים, מתן הנחיות לתיקון ליקויים לכל חברה שליקויים כאלה נמצאו במסגרת בחינת עמידתה בהוראות הדין ובהפקת הדוח המגזרי המסכם ופרסומו.

פיקוח הרוחב – נתונים על המגזרים והיקף הפיקוח

בשנת 2018 ביצעה הרשות 235 הליכי פיקוח רוחב לבדיקת היבטי הגנת הפרטיות ואבטחת המידע. פיקוחים אלו בוצעו בקרב המגזרים הבאים:

- 54 פיקוחי רוחב ייעודיים אשר התמקדו בבחינת קריטריון אבטחת המידע בלבד, והיוו פיילוט ראשוני לבחינת אופן ניהול המערך ככלי אכיפה משמעותי, במגזרי התיירות, בעמותות ואיגודים, מוסדות חינוך, ובחברות המספקות שירותים טכנולוגיים במסגרת הליך הבחירות לכנסת.
- 54 חברות המנהלות מאגרי מידע של מועדוני לקוחות בהיקפים של למעלה מ-100 אלף איש;
- 30 מרפאות לבריאות הנפש;
- 23 מכונים ומעבדות רפואיות;
- 38 ספקי פלטפורמות אינטרנטיות לימודיות אשר אוספות מידע על קטינים;
- 36 חברות המספקות שירותי אחסון ועיבוד מאגרי מידע;

בשנת 2019 ביצעה הרשות 244 פיקוחים. פיקוחים אלו בוצעו בקרב המגזרים הבאים:

- 70 רשויות מקומיות;
- 10 נותני שירותי סיוע במימוש זכויות רפואיות;
- 15 תאגידי מים ביוב וגז;
- 35 סוכנויות ביטוח;
- 14 מרכזי מוקדים טלפוניים;
- 40 בתי אבות;
- 40 חברות סיעוד;
- 20 הליכי פיקוח מעקב – אשר בחנו את אופן תיקון הליקויים ויישום ההנחיות שקבעה הרשות על-ידי הגופים שנדרשו לכך במסגרת הליך פיקוח הרוחב לשנת 2018.

בשנת 2020 ביצעה הרשות 224 הליכי פיקוח רוחב. בימים אלו מסתיים הליך פיקוח הרוחב אשר החל בשנת 2020 ומצוי בשלבי בחינת ממצאי פיקוחי המעקב ובחינת אופן תיקון הליקויים על-ידי הגופים שנדרשו לכך. פיקוחים אלו בוצעו במגזרים הבאים:

- 43 חברות כוח אדם והשמה;
- 49 גופים ממגזר הקוסמטיקה והכירורגיה הפלסטית;
- 51 קופות גמל וקרנות השתלמות;
- 31 גופים במגזר קמעונאות;
- 50 הליכי פיקוח מעקב – אשר בחנו את אופן תיקון הליקויים ויישום ההנחיות שקבעה הרשות על-ידי הגופים שנדרשו לכך במסגרת הליך פיקוח הרוחב לשנת 2019.

בשנת 2021 (נובמבר) יצאה הרשות ל-216 הליכי פיקוח רוחב, הליך הפיקוח צפוי להסתיים במהלך חודש מאי 2022. פיקוחים אלה מבוצעים בקרב המגזרים הבאים:

- 18 גופים במגזר התחבורה הדיגיטלית - אפליקציות תשלום מבוססי מיקום;
- 12 גופים במגזר אפליקציות בריאות דיגיטלית;
- 37 גופים במגזר התקשורת;
- 30 בתי חולים;

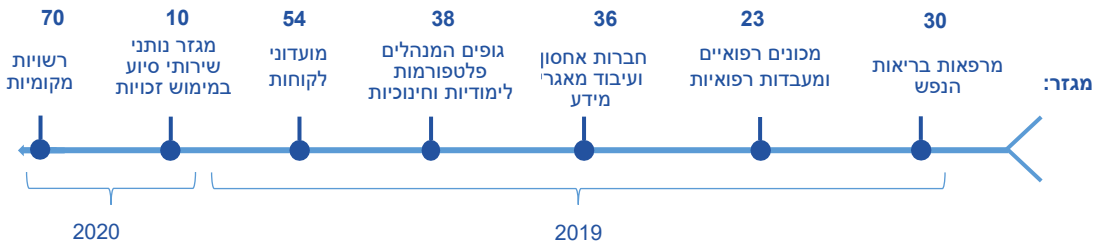
- 35 גופים במגזר עמותות ומגזר שלישי;
- כ-60 הליכי פיקוח מעקב – אשר יבחנו את אופן תיקון הליקויים ויישום ההנחיות שקבעה הרשות על-ידי הגופים שנדרשו לכך במסגרת הליך פיקוח הרוחב לשנת 2020;
- כ-24 פיקוחים מגזריים – אשר יבחנו בשנית מגזרים אותם כבר בחנה הרשות בעבר, אך יכללו בחינה של גופים אשר לא נבחנו במסגרת פיקוחי עבר אלה, זאת במטרה לבחון את אופן השפעת הליכי פיקוח הרוחב המגזריים על המשק ועל הגופים במגזרים שאותרו כמגזרים בעלי סיכון לפרטיות.

סיכום של פעילות פיקוח לפי שנים

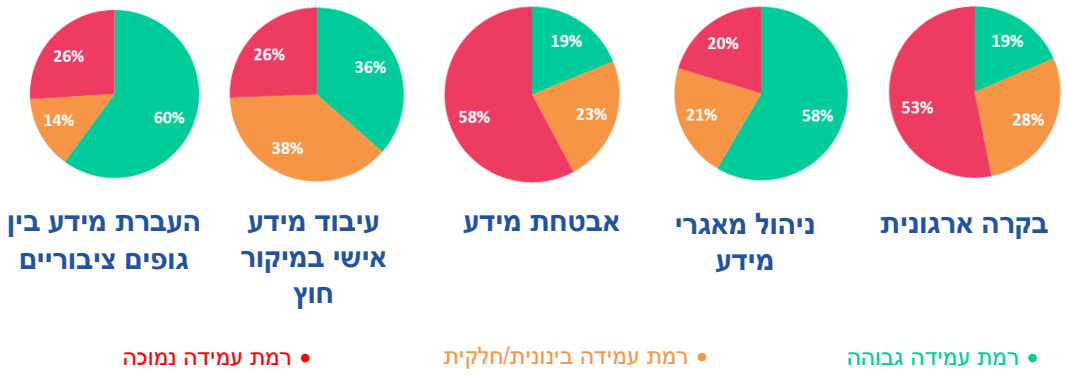
2018	מועדוני לקוחות	מרפאות לבריאות הנפש	פלטפורמות חינוך לקטינים	מכונים רפואיים ומעבדות רפואיות	חברות אחסון מאגרי מידע	פיילוט מוסדות חינוך, טכנולוגיות בחירות, תיירות, עמותות ואיגודים.	
2019	שירות סיעוד	מוקדים טלפוניים	סוכנויות ביטוח	מימוש זכויות רפואיות	תאגידי מים, ביוב וגז	בתי אבות	רשויות מקומיות
2020	חברות כוח אדם	תחום הקמעונאות	תחום שירותי הקוסמטיקה	קרנות ביטוח וקופות גמל			
2021	תחבורה חכמה	עמותות ומגזר שלישי	רפואה דיגיטלית	ספקי תקשורת	בתי חולים		

סיכום של פעילות פיקוח הרוחב במספרים

מספר גופים שנבדקו בקרב מגזרים בהם פורסמו דוחות מגזריים מתוך ממצאי הפיקוח



ממוצע רמות עמידה לפי קריטריונים



תהליך העבודה

בחירת יעדי פיקוח הרוחב מבוצעת במסגרת סקר שנתי הבוחן את סיכוני הפרטיות במגזרים השונים. במסגרת הסקר מזוהים מגזרים הכוללים שימוש במאגרי מידע בעלי רמת סיכון גבוהה יותר, בהתאם לגישה מבוססת סיכון בה נוקטת הרשות ביחס לכל הליבי האביפה שלה. להלן תיאור רמות הסיכון ומאפייני הסיכון המסייעים בבחירת יעדי הפיקוח:

הרשות להגנת הפרטיות מקיימת סקרי סיכונים שמבוססים על הערכות מצב עיתיות, ונוקטת בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש בפעולותיה על המשק, על מנת לעמוד במכלול האתגרים ולתעדף נכונה את משאביה. הרשות פועלת על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, בתחומים בהם ישנה השפעה רוחבית על מגזרים שונים, הכוללים מספר רב של משתמשים ומידע רגיש.

על יסוד ממצאי הסקר הרשות ממפה תופעות ומגזרים הכוללים סיכונים מיוחדים לפרטיות, ממקדת את תחומי העיסוק העתידיים שלה, ואת תשתית תכנית העבודה, הפעילות המחקרית, פרסום מדריכים, גילויי דעת והנחיות רגולטוריות, ואת פעילות האכיפה היזומה. בתוך כך, נבחרים גם המגזרים או התופעות בעלות הסיכון לפרטיות שייכללו בפעילות פיקוח הרוחב השנתית, תוך מיפוי הגופים בכל מגזר, ובניית מתודה תומכת לבחירת הגופים המפוקחים.

מיפוי רמות סיכון



סרגל סיכוני פגיעה בפרטיות	סיכון גבוה יותר לפרטיות	סיכון נמוך יותר לפרטיות
מהי כמות האנשים עליהם יש מידע	רבים	מעטים
מהי כמות המידע שנשמר על כל אדם	רב	מועט
מהי רגישות המידע הנשמר	גבוהה	נמוכה
מה משך זמן השמירה של המידע	ללא הגבלת זמן	זמן קצר
מהי כמות המידע שמועבר	רבה	לא מועבר
מה כמות הממשקים החיצוניים למערכת המידע	רבים	ללא ממשקים
מה הסיכוי לנזק ממשי מגילוי המידע	גדול	לא קיים או נמוך
האם המידע מקושר באופן חזק לזהות	קישור חזק לזהות	קישור חלש או ללא קישור
האם ניתן לעשות במידע שימוש אחר	ניתן	לא ניתן
האם האנשים מודעים לשימוש במידע	לא מודעים	מודעים
האם איסוף המידע נעשה בהסכמת אנשים	לא	כן
האם השימוש במידע נעשה בהסכמת אנשים	לא	כן

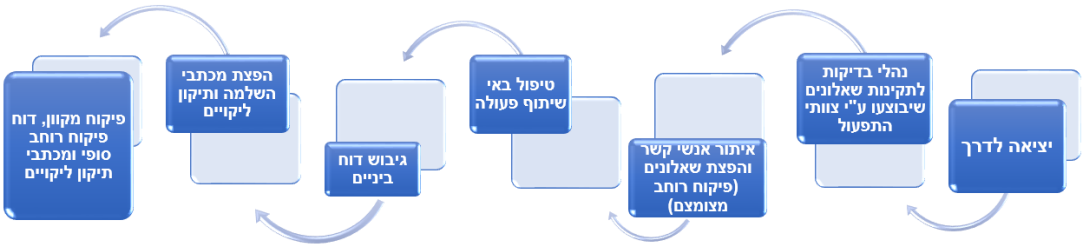
תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בשלב בניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לתכנית העבודה השנתית של הרשות, ובהתחשב בבחינת כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע לאותו מגזר/נושא, תלונות ספציפיות שהתקבלו ברשות, והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

עם סיום בניית תכנית העבודה והתאמת נהלי העבודה לניהול ההליך, מתחיל הליך הפיקוח עצמו. ההליך כולל, בין השאר, הפצת שאלונים מותאמים למגזר ולסיכונים המיוחדים שהוא כולל, קבלת מענה לשאלונים מהגופים וגיבוש דו"ח ביניים פנימי, הוצאת דרישה להשלמת מידע מגופים רלוונטיים, פיקוח מדגמי במשרדי המפוקחים, גיבוש דו"ח סופי פנימי, מתן הנחיה לתיקון הליקויים אם נמצאו בגוף המפוקח ופרסום דו"ח מגזרי לציבור.

בנוסף, מבצעת הרשות פיקוחי מעקב באופן מדגמי על חלק מהגופים שנבדקו בכדי לוודא את יישום דרישות תיקון הליקויים. ביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, רשאית הרשות להטיל סנקציות נוספות העומדות לרשותה מכוח החוק.

בגופים שלא ישתפו פעולה או שבהם נמצאו ליקויים חמורים במילוי הוראות החוק, עשויה הרשות להפעיל את סמכויותיה המנהליות או הפליליות לשם בחינת החשדות להפרת החוק.

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיוצרת פעילות פיקוח הרוחב על המגזרים שנבדקו, בוחנת הרשות אם חל שינוי ברמת הציות להוראות החוק, על ידי בחינת גופים נוספים במגזרים אלה והשוואת תוצאותיהם לאלה של הגופים אשר נבחנו בהליך הפיקוח הראשי.



עם תחילת הליך הפיקוח, נדרשים הגופים במגזרי הפיקוח להשיב על שאלוני ביקורת ולספק נתונים שונים לבחינת עמידתם בהוראות החוק והתקנות, בין היתר בהתייחס לאופן קבלת ההסכמה לשימוש במידע האישי בו הם מחזיקים, אופן השימוש בו, עיבודו ורמת אבטחתו.

כל אחד מהגופים נדרש למלא שאלוני ביקורת לבחינת עמידתו ב-4-5 קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע, אבטחת מידע ושימוש בשירותי מיקור חוץ. בנוסף, בחלק מהגופים נבדק קריטריון נוסף של העברת מידע בין גופים ציבוריים. הציונים ניתנים לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות החוק ובתקנות מכוחו.[1]

[1] קריטריון "העברת מידע בין גופים ציבוריים" רלוונטי לגופים ציבוריים לפי צו הגנת הפרטיות (קביעת גופים ציבוריים) תשמ"ו-1986

הקריטריונים הנבדקים ואופן קביעת רמת העמידה בהוראות החוק והתקנות מכוחו:

במטרה לבחון את רמת העמידה של הגופים המפוקחים בהוראות החוק והתקנות, מתייחסים שאלוני ביקורת לקריטריונים שונים ובהם:

קריטריון זה בוחן את אופן העמידה בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול מאגרי המידע האישי שבבעלותם ובהחזקתם.

קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום.

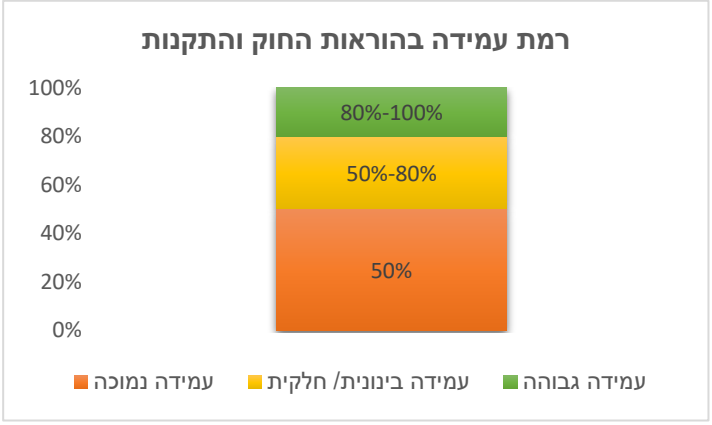


בחינת ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים את ההגנה על המידע.

בחינת קיומן של ועדות הבוחנות את הצורך בהעברת המידע, אי העברת מידע עודף, הסמכות להעברה וקבלת מידע מגופים ציבוריים ואליהם ובחינת רמת האבטחה בגוף הנעבר.

מגזרים מסוימים מעלים סיכונים ייחודיים אשר גם הם יכולים להיכלל במסגרת הבחינה. כך לדוגמה במגזר הרשויות המקומיות נבחן קריטריון ניהול מאגרי מצלמות מעקב במרחב הציבורי – לרבות אופן היידוע והשימוש של הרשויות המקומיות במצלמות מעקב במרחב הציבורי, העמידה בהוראות הרשם וכד'.

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.



רמת העמידה בהוראות החוק והתקנות נקבעת בהתאם לשקלול הציונים שקיבלו הגופים המפוקחים, וזאת בהתבסס על בחינת הרשות את מענה הגופים לשאלוני הביקורת, הראיות והמידע שנאסף במסגרת ההליך.

המגזרים שנבדקו, רקע, מאפיינים וסיכונים:

כאמור הדו"ח מרכז ומסכם את 7 הדוחות שפורסמו עד כה לציבור ביחס ל-7 המגזרים הבאים:

בהליך פיקוח רוחב זה פנתה הרשות בדרישה למילוי שאלון ביקורת ל-70 רשויות מקומיות המנהלות מידע אישי על למעלה מ-5,000,000 תושבים, ביניהן נכללות 33 רשויות גדולות הכוללות למעלה מ-42,000 תושבים, 10 רשויות בינוניות הכוללות בין 30,000 ל-42,000 תושבים ו-27 רשויות קטנות יותר הכוללות בין 3,000 ל-30,000 תושבים.

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל-10 גופים המעניקים שירותי סיוע במימוש זכויות רפואיות, כאשר במסגרת בחירת הגופים נלקחו בחשבון היקפי המידע וכמות הלקוחות, ורגישות המידע במסגרת השירותים הניתנים ללקוחות.



בהליך פיקוח רוחב זה פנתה הרשות ל- 54 גופים המנהלים מועדוני לקוחות. בניכוי גופים אשר סיימו פעילותם, שינו פעילות, דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, ולאחר איחוד גופים אשר השיבו מענה מאוחד בשל פעילות עסקית או טכנולוגית מאוחדת, בפועל נמצאו תחת פיקוח 44 גופים.

במסגרת הליך זה פנתה הרשות ל-30 גופים המנהלים מרפאות לבריאות הנפש, כאשר בניכוי גופים אשר סיימו פעילותם, שינו את תחום הפעילות או דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, או השיבו באופן מאוחד בשל פעילות או תשתית טכנולוגית משותפת, התמקד הליך הפיקוח ב-18 גופים אשר נבדקו במסגרת הפיקוח במגזר זה.

בהליך פיקוח רוחב זה הרשות פנתה בדרישה למילוי שאלוני ביקורת ל-38 גופים המנהלים מידע אודות קטינים באמצעות פלטפורמות לימודיות.

במסגרת הליך זה שלחה הרשות שאלונים ל-23 גופים המנהלים מכונים רפואיים, כאשר בניכוי גופים אשר סיימו פעילותם, שינו פעילות, או דיווחו על פעילות שאינה רלוונטית למגזר זה, נבדקו במסגרת הליך הפיקוח 20 גופים.

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 או טכנולוגית מאוחדת, נמצאו תחת הליך הפיקוח 26 גופים.

מחד, מגזרי הפיקוח שונים מבחינת היקפי המידע הרגיש, האופן שבו מתקבל אצלם המידע ופערי הכוחות בין נותני השירות ונושא המידע, אך מאידך, נמצאו סיכונים משותפים למגזרים אלו הנובעים בין היתר מהסיכונים הנגרמים בהסתמכות על שירותי מיקור חוץ, היכולת לבצע הצלבת מידע בין מאגרי מידע, וכמובן סיכוני אבטחת מידע שנלווים לכמות מידע גדולה ולהיקף מידע רגיש.

מגזר רשויות מקומיות [2]



במסגרת סקר שבחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר הרשויות המקומיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה. המאפיינים בייחודיים נובעים מעצם היותה של רשות מקומית גוף ציבורי הכפוף להוראות חוק ייחודיות, יחסי האמון בין הרשות המקומית לבין התושב, וכן בהיבטי פרטיות הבאים לידי ביטוי בניהול והחזקת מידע רחב ורגיש אודות תושבי הרשות המקומית. מידע זה כולל בין היתראת מרשם התושבים, מצב הנכסים ובעליהם, מצב גבייה ואכיפת גבייה, מידע אודות תלמידים, מטופלים על ידי לשכות הרווחה, פירוט ספקי העירייה ונתונים כספיים בהתקשרות עימם ואף מידע אודות יעוץ פסיכולוגי וסוציאלי.

גורמי סיכון לפרטיות נוספים במגזר זה נובעים מעצם היותן של רשויות מקומיות בעלים של מאגרי מידע רבים הניתנים להצלבה, ומהיכולת שלהן לעשות שימוש במידע הקיים ברשותן לצרכים שונים; שימוש רב בנותני שירותים חיצוניים לרשות המקומית דבר אשר מאפשר, במצבים מסוימים, חשיפה למידע רגיש הקיים במאגרי הרשות; היותן של רשויות מקומיות גופים ציבוריים המוסרים ומקבלים דרך קבע מידע אישי על תושבים מגופים אחרים, מנגנוני מחשוב גדולים שעשויים לייצר גישה למידע למספר רב של מורשי גישה, וכן נוכח פרסומי עבר של דוחות מבקר המדינה מהשנים 2012, 2017 ו-2020 אשר בחנו היבטים שונים בתחום מערכות המידע וכללו בין היתר הערות לגבי מידת המענה הניתן על ידי הרשויות המקומיות לחוק הגנת הפרטיות ותקנותיו.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותן רשויות מקומיות לעמוד בדרישות החוק והתקנות ביתר שאת בהגנה על פרטיות התושבים, לרבות קיום חובות אבטחת המידע, קיום חובת השקיפות כלפי נושא המידע, התקשרות תקינה מול מעבדי מידע במיקור חוץ, ניהול תקין של העברות מידע בין גופים ציבוריים, שימוש כדין במצלמות מעקב במרחב הציבורי, וקיום בקרה ארגונית.

נוכח כל אלה הגדירה הרשות להגנת הפרטיות מגזר זה כיעד פיקוח רוחב משמעותי. פיקוח הרוחב התמקד בעיקר באופן ניהול המידע ברשויות בנושאי גבייה, חינוך ומצלמות אבטחה.

מגזר מועדוני הלקוחות בישראל [3]



מגזר זה מנהל ומחזיק מאגרי מידע רבים המתייחסים למידע רגיש ומזוהה אודות הרגלי צריכה, ומנהל קשר אינטראקטיבי עם ציבור לקוחותיו, בין אם באופן ישיר ובין אם באמצעות שירותי מיקור חוץ. ניהול הקשר עם הלקוחות הכולל שימוש במידע רגיש בהיקף נרחב, מחייב את מועדוני הלקוחות לעמוד בדרישות אבטחת המידע, לקיים את חובת השקיפות אל מול הלקוח (ובכלל זה למסור ללקוח כי הוא אינו חייב למסור את המידע אם אין חובה חוקית לכך), ולעמוד בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר.

---

[2] דו"ח ממצאי הליך פיקוח רוחב בקרב רשויות מקומיות - דו"ח ממצאי הליך פיקוח רוחב בקרב רשויות מקומיות
[3] דוח ממצאי פיקוח רוחב בקרב מגזר מועדוני לקוחות - דוח ממצאי פיקוח רוחב בקרב מגזר מועדוני לקוחות

גופים המנהלים פלטפורמות לימודיות וחינוכיות לקטינים [4]



מגזר הגופים המנהלים אתרים ואפליקציות לימודיות וחינוכיות המיועדות לקטינים (ובקצרה "פלטפורמות לימודיות"), מתאפיין בין היתר בפערי כוחות משמעותיים בין הפלטפורמות הלימודיות האוספות את המידע לבין הקטין עצמו. מאפיין מיוחד 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, הישגים לימודיים, תמונות ועוד.

מגזר חברות אחסון ועיבוד מאגרי מידע [5]



מגזר חברות אחסון ועיבוד מאגרי מידע בישראל מחזיק מאגרי מידע רבים המכילים מידע רגיש ומזוהה. לעניין זה מגדיר החוק "מחזיק, לעניין מאגר מידע" - מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". הגדרה 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 הרוחב מעניקות שירותים שונים עבור בעלי מאגרי מידע שונים. בין היתר, שירותי תוכנה או פלטפורמה PAAS – Service as a Platform, SAAS - Service a as (Software) הכוללים אפליקציות, ממשקים ופיתוחים עבור בעלי מאגר המידע הניתנים על-ידי מחזיק מאגר המידע המספק שירותים אלו, לרבות אירוח אתרי אינטרנט הכוללים מידע אישי. חלק מהחברות מעניקות שירותי תשתית (IAAS – Service a as Infrastructure), הכוללים מתן שירותי אחסון על ידי מחזיקים עבור בעלי מאגרי המידע.

ניהול מידע של מספר לקוחות על גבי אותה פלטפורמה, היקפי המידע, ומספרם הרב של האנשים עליהם מוחזק המידע, דורשים הקפדה מיוחדת על עמידה בהוראות החוק והתקנות. ניהול והחזקת מידע אישי מחייבים את חברות אחסון ועיבוד המידע לעמוד בדרישות החלות על "מחזיקים" 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 החוק הכוללות, בין היתר, מינוי ממונה על אבטחת מידע וחובת דיווח לרשות להגנת הפרטיות מדי שנה על המאגרים הנמצאים ברשותם, ניהול ההרשאות בהם, וציון שמם של בעלי המאגרים.

---

[4] דוח ממצאי פיקוח רוחב בקרב מגזר ספקי פלטפורמות אינטרנטיות לימודיות אשר אוספות מידע על קטינים בישראל דוח ממצאי פיקוח רוחב בקרב מגזר ספקי פלטפורמות אינטרנטיות לימודיות אשר אוספות מידע על קטינים בישראל

[5] דוח ממצאי הליך פיקוח הרוחב בקרב מגזר חברות המספקות שירותים של אחסון ועיבוד מאגרי מידע אישי דוח ממצאי הליך פיקוח הרוחב בקרב מגזר חברות המספקות שירותים של אחסון ועיבוד מאגרי מידע אישי

מכונים רפואיים ומעבדות רפואיות [6]





הרשות להגנת הפרטיות הגדירה את מגזר המכונים הרפואיים והמעבדות הרפואיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה. אלו כוללים, בין היתר, את אופי היחסים בין הגוף המטפל והמטופל, אשר נדרש למסור מידע רגיש אודות מצבו הבריאותי, או שמידע כאמור נאסף תוך כדי הטיפול. מדובר, בין היתר, במידע רפואי דוגמת אבחוני שמיעה, קלינאות תקשורת, הדמיה ופיזיותרפיה, פוריות, ממוגרפיה, דיאליזה, התפתחות הילד ומידע אודות מצב נפשי. במסגרת יחסים אלו המטופל לא בהכרח מודע לאופן השימוש במידע אודותיו והעברתו לגורמים אחרים. בנוסף, ניהול ואחזקת המידע אודות מצבם הבריאותי של המטופלים מבוצע באופנים שונים, לרבות באמצעות מיקור חוץ, או באופן ישיר ובאמצעות מאגרי קופות החולים, והכל בהיקפי מידע גדולים וברמת רגישות גבוהה.

מגזר מרפאות בריאות הנפש [7]





מגזר מרפאות בריאות הנפש, אשר נבחן במסגרת דו"ח זה, כולל מרפאות שמעניקות שירותי טיפול נפשי בבתי חולים כלליים, בתי חולים לבריאות הנפש ומרכזים ייעודיים לבריאות הנפש. כמו במגזר הקודם, מרפאות בריאות הנפש מחזיקות במידע רפואי רגיש ביותר על מצבם הנפשי של מטופלים ובהיקפים גדולים. כמו כן, במגזר זה קיימת מערכת יחסים ייחודית בין הגופים המטפלים לבין ציבור המטופלים אשר לעיתים, בשל מצבם הרפואי, אין ביכולתם להעניק את הסכמתם למסירת מידע אודותיהם או שהוא נאסף תוך כדי הטיפול בהם. אופן הניהול ואחזקת המידע אודות מצבם הבריאותי של המטופלים מתבצע באופן שונה בקרב המרפאות השונות. יש שמנהלות את המידע באופן עצמאי ויש המסתייעות בשירותי מיקור חוץ.

ניהול המידע הרגיש הכולל מידע דמוגרפי, רפואי גנטי ומידע על מצב נפשי עלולים להפוך אותו ליעד תקיפה "אטרקטיבי" לאירועי אבטחת מידע, בין אם על ידי בעלי הרשאות גישה למאגר המידע ובין אם על ידי פצחנים (האקרים) העלולים לבצע שימוש לרעה במידע ואף להשתמש בו כאמצעי סחיטה.

---

[6] דוח ממצאי פיקוח רוחב בקרב מכונים רפואיים ומעבדות רפואיות בישראל - דוח ממצאי פיקוח רוחב בקרב מכונים רפואיים ומעבדות רפואיות בישראל

[7] דוח ממצאי פיקוח רוחב בקרב מגזר מרפאות בריאות הנפש בישראל - דוח ממצאי פיקוח רוחב בקרב מגזר מרפאות בריאות הנפש בישראל

מגזר נותני שירות סיוע במימוש זכויות רפואיות [8]



במסגרת סקר שערכה הרשות להגנת הפרטיות לבחינת סיכוני הפרטיות במגזרים השונים, אותר מגזר הארגונים העוסקים בשירותי סיוע במימוש זכויות רפואיות בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים.

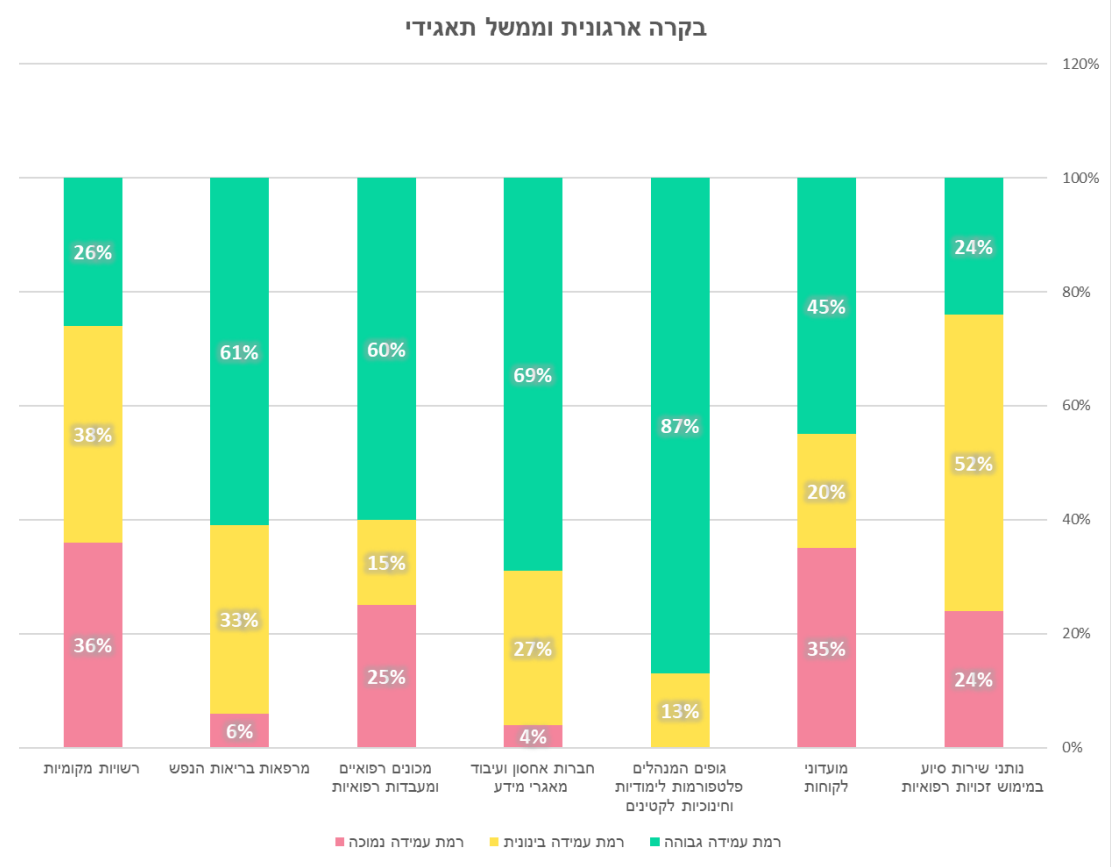
הגופים במגזר זה מעניקים שירותי סיוע במימוש זכויות רפואיות מול רשויות המדינה השונות עבור לקוחותיהם, ובתוך כך מקבלים לידיהם מידע רב ורגיש, לעתים בעל מאפיינים ייחודיים, המהווה סיכון בהיבטי הפרטיות. מאפיינים אלו באים לידי ביטוי במערכת יחסים מיוחדת ופערי כוחות מובנים בין נותן השירות לבין נושא המידע, אשר מוסר מידע רגיש לרבות מידע אודות מצבו הבריאותי, הנפשי הכלכלי וכדומה, ואף מעניק הרשאות גישה רחבות ושימוש במידע על אודותיו, מבלי שיהיה מודע בהכרח לאופן השימוש במידע ולהעברתו לגורמים אחרים. מאפיין נוסף של מגזר זה הוא עצם ניהול והחזקת כמויות גדולות של מידע רפואי רגיש בידי גופים פרטיים.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותם ארגונים לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית, ועמידה בהוראות החוק בכל הנוגע לדיווח ישיר ולשירותי דיווח ישיר. נוכח כל אלה הגדירה הרשות להגנת הפרטיות מגזר זה כיעד פיקוח רוחב משמעותי.

[8] דוח ממצאי פיקוח הרוחב בקרב נותני שירותי סיוע במימוש זכויות רפואיות דוח ממצאי פיקוח הרוחב בקרב נותני שירותי סיוע במימוש זכויות רפואיות

השוואת רמת העמידה בין המגזרים השונים שנבדקו ביחס לקריטריונים זהים

בקרה ארגונית - רמות עמידה לפי מגזר



ברוב מגזרי הפיקוח שנבחנו נמצאו פערים בקריטריון זה אשר בוחן את קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום. חלק מהפערים מיוחסים לאי מינוי מנהלי מאגר מידע או להעדר כתבי מינוי של מנהלי מאגר מידע.

במגזרים הכוללים מידע רפואי, כגון מגזר מימוש זכויות רפואיות, מכונים רפואיים ומעבדות וכן מרפאות בריאות הנפש, נמצא כי נהלי אבטחת המידע אינם מכסים באופן מלא את הדרוש על פי תקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע) בגון הוראות בדבר האבטחה הפיסית והסביבתית של המאגר, הרשאות גישה, תיאור אמצעי הגנה ואופן הפעלתם והוראות למורשי הגישה לצורך שמירתו, ואף נמצאו גופים בהם כלל לא קיימים נהלי אבטחת מידע. פערים מהותיים נמצאו גם בתחום תהליכי מתן הרשאות גישה לעובדים חדשים או הענקת גישה למערכות המאגר. פיקוחי הרוחב העלו כי אלו אינם עוברים תהליך מיון ולא נבדקת התאמתם לקבלת הגישה למאגרי המידע, או שהליכי המיון והדרכות העובדים אינם נעשים כנדרש בחוק ובתקנות. חשוב לציין כי בדומה למגזרי הבריאות, גם במגזר הרשויות המקומיות נמצאו פערים דומים.

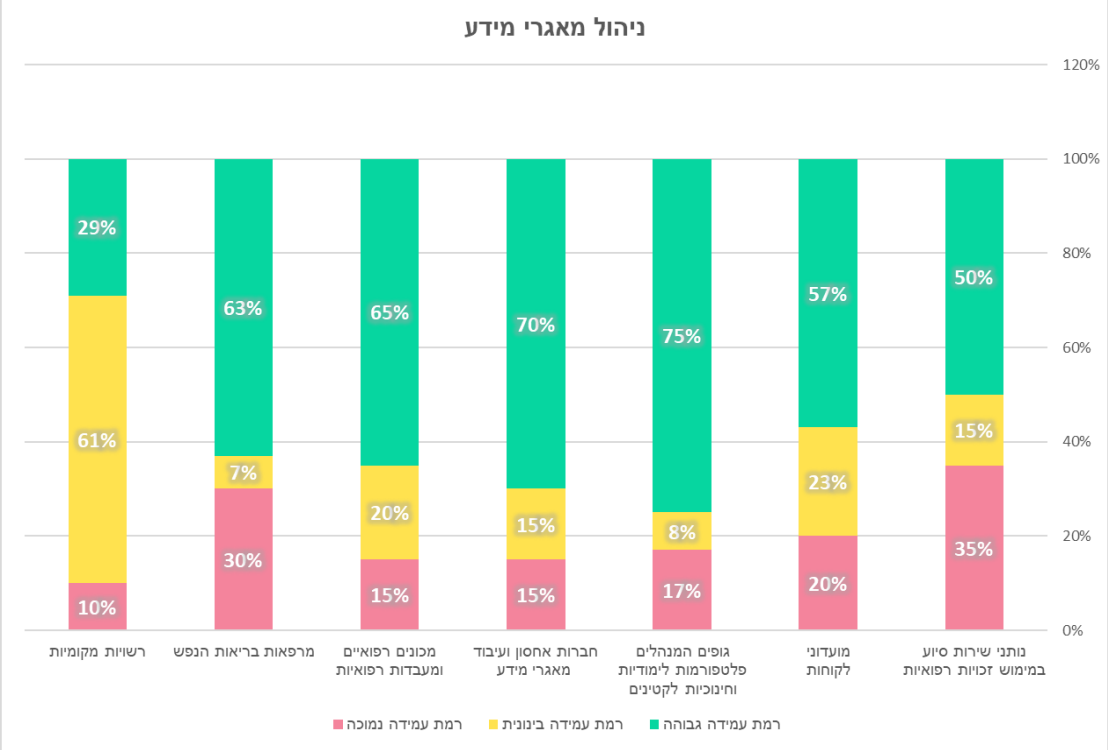
עוד נציין, כי ביקורת תקופתיות וסקרי סיכונים לא בוצעו באופן מלא הן במגזר הרשויות המקומיות והן במגזרי הפלטפורמות הלימודיות לקטינים, מכונים ומעבדות רפואיות, וחברות האחסון. נדגיש כי ליקוי זה בקרב חברות האחסון חמור במיוחד, שכן קיימת הסתמכות כמעט מלאה על הבקרות שמבצעת חברת האחסון, אשר מתוקף פעילותה מחזיקה ומעבדת מידע עבור אחרים. ביקורת תקופתית וסקרי סיכונים הינם מרכיב מהותי אשר מסייע בהפחתת החשיפה לדלף מידע. נזכיר כי בהתאם להוראת

סעיף 17 לחוק הגנת הפרטיות, בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, נושאים כולם באחריות מלאה לאבטחת המידע שבמאגר.

בהקשר זה הבהירה הרשות בדוח ממצאי הליך פיקוח הרוחב בקרב מגזר חברות האחסון את עמדתה ולפיה חברה 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 ביד החברה אלא נשמר 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.

לפי ממצאי פיקוח הרוחב ניתן לראות כי באופן יחסי בקריטריון הבקרה הארגונית נמצאה רמת עמידה בינונית-נמוכה בהוראות הדין. במגזרים הטכנולוגיים או הרפואיים המצויים תחת רגולציה מקבילה, נמצאה רמת עמידה גבוהה יותר בקריטריון זה מאשר במגזרים האחרים.

ניהול מאגרי מידע - רמות עמידה לפי מגזר



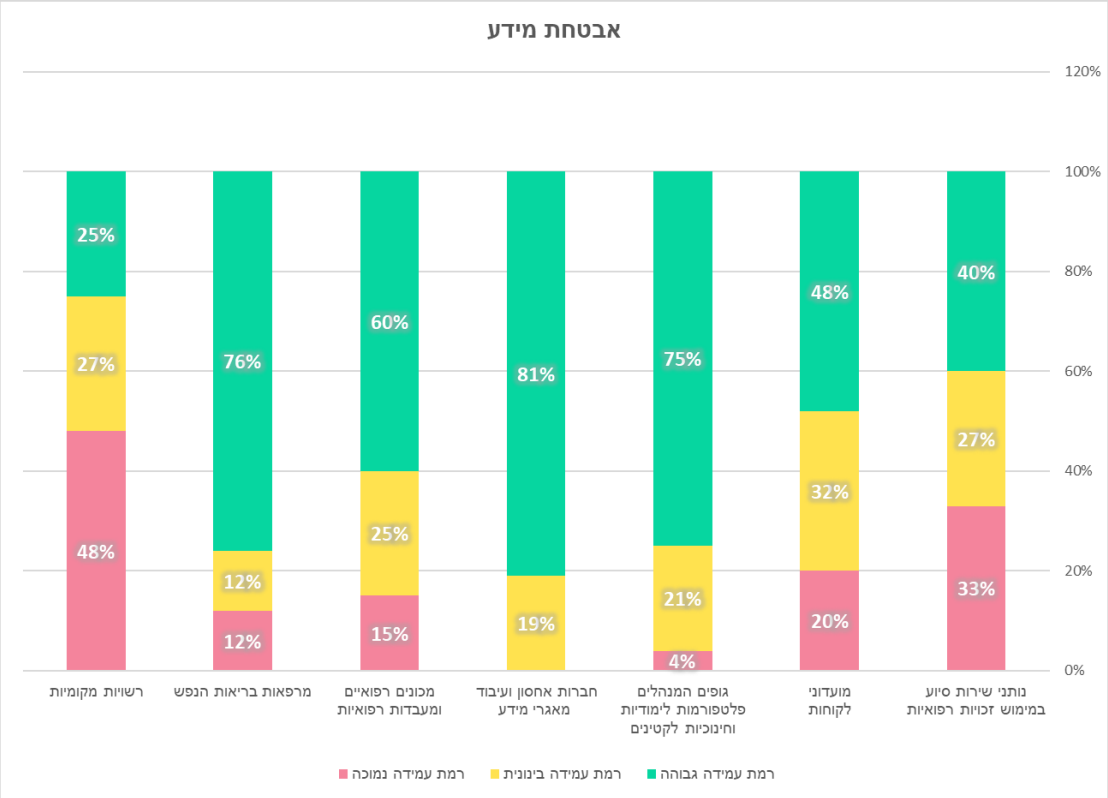
נראה כי קיים מתאם מסוים בין גודל הגוף המפוקח למידת יישום הוראות החוק בעת בחינת הקריטריון של ניהול מאגרי מידע, הבוחן את אופן קבלת ההסכמה לשימוש במידע אישי, האם השימוש במידע תואם את המטרה שלשמה נאסף, מתן זכות העיון במידע, עמידה בהוראות החוק בעניין דיוור ישיר וביוצ"ב.

במגזר הרשויות המקומיות ובמגזר הגופים המנהלים פלטפורמות לימודיות וחינוכיות לקטינים, וכן במגזר מכונים ומעבדות רפואיות נמצאה רמת עמידה בינונית-נמוכה בקריטריון זה. כמו כן, נמצא פער משמעותי בין רמת עמידתם הגבוהה יחסית של גופים גדולים ממגזרים אלו בהוראות חוק הגנת הפרטיות והתקנות, לבין גופים קטנים אשר רמת עמידתם בהוראות החוק והתקנות נמצאה נמוכה יחסית. בגופים אלו נמצאו ליקויים עיקריים שנבעו מטיפול בלתי נאות בתהליך איסוף המידע והיעדר אפשרות לעיין או לתקן מידע על ידי נושא המידע. ממצאים דומים נמצאו גם במגזר מועדוני הלקוחות.

במגזרים הכוללים מידע רפואי - מגזר נותני שירותי סיוע במימוש זכויות רפואיות ומגזר בריאות הנפש - נמצאו פערים בנושא מתן הודעה לנושא המידע בעת איסוף המידע שלא בהתאם לדרישות סעיף 11 לחוק הקובע חובה על ציון אם חלה חובה חוקית למסור את המידע, פירוט מטרת איסוף המידע ולמי יימסר המידע ולאילו מטרות. נמצאו גם פערים בשימוש נוסף במאגר המידע שלא למטרה לשמה הוקם, וכן נמצא כי חלק מהגופים אינם שומרים או מתעדים את אופן קבלת הסכמת נושאי המידע למסירת המידע ויידועם בדבר הזכויות המוקנות להם מכוח החוק. נמצאו גופים אשר לא אפשרו לנושאי המידע לשנות או לתקן את המידע המוחזק אודותיהם כנדרש בחוק. נציין כי קיימת חשיבות יתרה לאפשר לנושאי המידע לתקן את המידע האישי אודותיהם, אם אינו נכון, שלם, ברור או מעודכן, בפרט כשמדובר על מידע רפואי והיסטוריה רפואית.

לפי ממצאי פיקוח הרוחב ניתן לראות כי רמת העמידה הקיימת בקריטריון הינה בינונית-גבוהה, ועל פי ממצאי פיקוחי המעקב, חלק גדול מהגופים פעלו לתיקון הליקויים בקריטריון זה.

אבטחת מידע - רמות עמידה לפי מגזר



נמצאה רמת עמידה נמוכה-בינונית על פי קריטריון אבטחת המידע הבוחן את אופן העמידה בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בקרב מגזר הרשויות המקומיות, מגזר נותני שירותי סיוע במימוש זכויות רפואיות ומגזר מועדוני הלקוחות, המהווים מבחינה מספרית מעל 50% מהגופים המפוקחים, 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. בנוסף, נמצאו ליקויים רבים בנושא אבטחת אמצעים נתיקים כגון Disk On Key בין אם בהעדר הגבלות על שימוש באמצעים אלו או בהעדר הצפנה נאותה. בקרב גופים רבים אף לא גובש נוהל עבודה סדור לטיפול באירועי אבטחת מידע.

ניכר כי נושא אבטחת המידע דורש טיפול באופן נרחב בקרב הגופים המפוקחים.

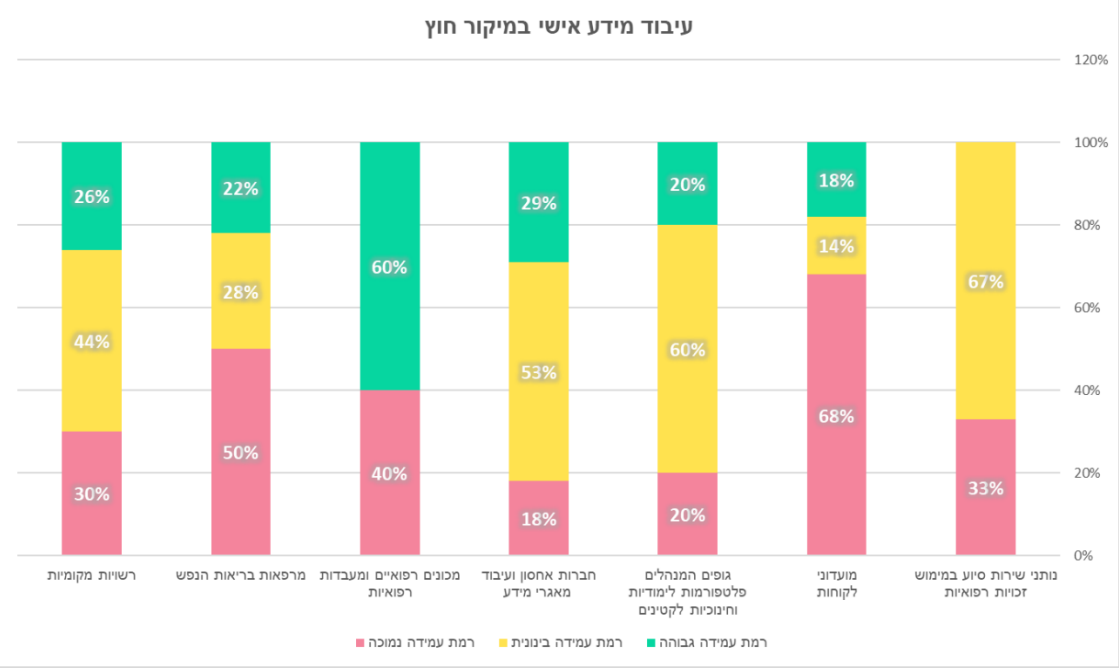
ביחס לגופים המנהלים פלטפורמות לימודיות וחינוכיות לקטינים, מרבית הגופים שנבדקו מחזיקים את מאגרי המידע בענן ובחוות שרתים שונות, המספקים שירותי אבטחת מידע שונים. כפועל יוצא טוענים הגופים כי הם עומדים בתנאי האבטחה הנדרשים בחוק, בעוד שלמעשה נדרשת רכישה של שירותי אבטחה ספציפיים מחוות השרתים או נקיטת צעדי אבטחה עצמאיים באופן מקיף יותר, בכדי לעמוד בהוראות תקנות הגנת הפרטיות (אבטחת מידע). הנחה זו שבה וחזרה במסגרת הליכי פיקוח הרוחב בקרב גופים ממגזרים נוספים.

כמו כן, גופים רבים העומדים בתקן ISO27001 סברו בטעות שהינם פטורים מיישום התקנות והליכי הפיקוח. בעניין זה הבהירה הרשות במסגרת הנחיית רשם מאגרי המידע מס' 03/2018 כי רק ארגון אשר מחזיק בתעודת הסמכה לתקן וגם מקיים בפועל את הוראותיו, לרבות כל הבקרות הרלוונטיות - יראו בו ככזה המקיים את תקנות הגנת הפרטיות (אבטחת מידע) ביחס למאגרים לגביהם ניתנה

ההסמכה לתקן. ההנחיה לא תחול על ארגון אשר הרשות מצאה כי אינו מקיים בפועל את הוראות התקן, גם אם הוא מחזיק בתעודת הסמכה. [9]

לפי ממצאי פיקוח הרוחב בקריטריון זה ניתן לראות כי אופן הציות המגזרי בכל הנוגע לאבטחת המידע דינמי, ותלוי מגזר או גוף. מן הממצאים עולה תמונה מדאיגה בה קיימים ליקויים באבטחת המידע, הן במגזרים המנהלים מידע רגיש במיוחד כדוגמת גופים המעניקים שירותים רפואיים, והן במגזרים המנהלים כמויות עצומות של מידע כגון רשויות מקומיות או גופים הכוללים מאגרי מועדון לקוחות.

עיבוד מידע אישי במיקור חוץ - רמות עמידה לפי מגזר



נושא עיבוד מידע אישי במיקור חוץ הבוחן בין היתר את אופן ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע, נמצא לוקה בחסר באופן מובהק **בכלל המגזרים שבוצע בהם פיקוח הרוחב**. כ-75% מהגופים לא עומדים באופן מלא בהנחיות הרשות בעניין זה. מרבית הליקויים נמצאו בנושאים של היערכות להתקשרות עם ספק מיקור חוץ לשם מתן שירותי עיבוד מידע אישי, אופן עיבוד המידע האישי במיקור חוץ, ופעולות מספקות בכדי לוודא שספק מיקור החוץ נוקט באמצעים הנדרשים כדי להגן על מאגרי המידע.

[9] ראו הנחיית רשם מאגרי המידע מס' 3/2018 - תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, על ארגונים המוסמכים לתקן ISO/IEC 27001 - הנחיית רשם מאגרי המידע מס' 3/2018 - תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, על ארגונים המוסמכים לתקן ISO/IEC 27001

ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בארגון ועמדו ברמה גבוהה 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 דרך קבע או העברתו למיקור חוץ אינם בגדר מסירת מידע למחזיק במאגר כאמור בהוראות החוק, וכתוצאה מכך 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 מכך. מרבית הגופים נמצאו ככאלה שאינם מבצעים התקשרות עם ספק מיקור חוץ לפי הוראת תקנה 15 לתקנות 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.[10]

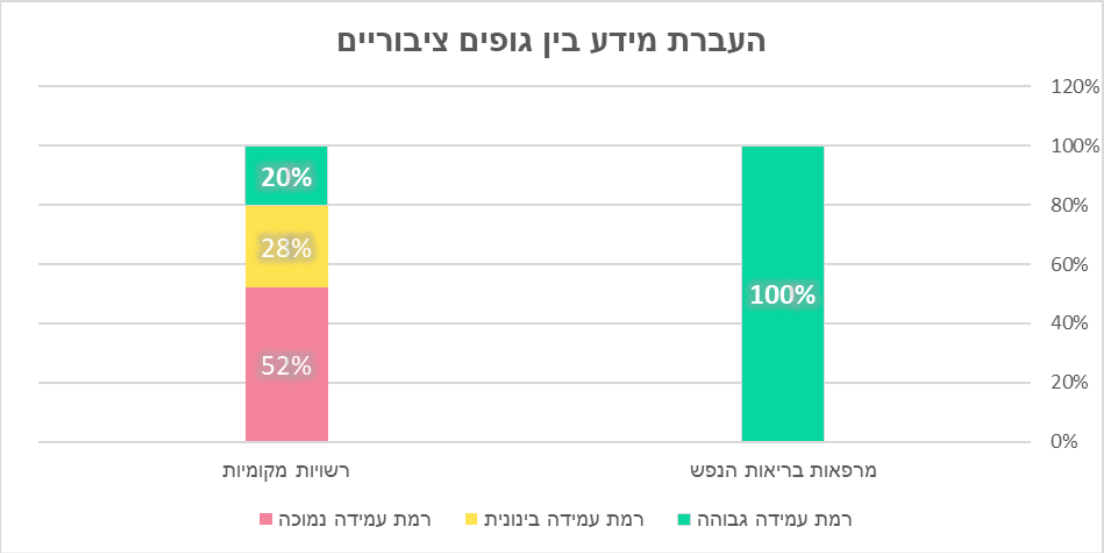
נציין כי בקרב חברות האחסון ליקוי זה מתבטא בכך שהגופים בהם נמצאה רמת עמידה בינונית או נמוכה, לא נקטו צעדים מספקים מבעוד מועד על מנת להעריך את מידת הסיכון הנשקפת למידע, ולפגיעה בזכותם לפרטיות של נושאי המידע, כפועל יוצא מהשירותים הניתנים על ידם, או בשימוש של הגופים עצמם במיקור חוץ בכל הנוגע לעיבוד ואחסון מידע. בין היתר נמצא כי חלק מהגופים לא עומדים בתנאי ההתקשרות הנדרשים לפי תקנה 15 לתקנות כלפי ספקי מיקור חוץ נוספים בצורה מספקת, אינם בוחנים את איכות ניהול אבטחת המידע ואופן תפעול מאגרי המידע אצל ספקי מיקור החוץ, ואינם מבצעים פעולות פיקוח כנדרש. מדובר בתמונת ראי של יישום התקנות בקרב גופים המקבלים שירותי עיבוד מידע אישי במיקור חוץ.



לפי ממצאי פיקוח הרוחב ניתן לראות כי רמת העמידה בקריטריון זה הינה בינונית, ולמעשה היא מצביעה באופן עקבי על ציות נמוך בקרב כלל המגזרים שנבדקו לאורך פעילות פיקוח הרוחב, בכל הקשור לחובות בדין הנוגעות לעיבוד מידע במיקור חוץ. באופן רוחבי, נראה כי ליקויים אלו חוזרים על עצמם, הן בשל חוסר המודעות של הגופים המנהלים את המאגרים לחובותיהם במסגרת התקשרות עם גורמים שלישיים, והן מחוסר המודעות של גופים המעבדים מידע במיקור חוץ לחובות החלות עליהם. יצוין, כי מסקנות בכל הקשור לעמידת מנהלי המאגרים בקריטריון זה, ניתן לראות בכל דוחות פיקוח הרוחב שפרסמה הרשות, ובאופן פרטני בדו"ח מגזר חברות אחסון ועיבוד מאגרי מידע המפרט את חובתם של מעבדי המידע.

[10] ראו דוח פיקוח רוחב - ממצאי הליך פיקוח הרוחב בקרב מגזר חברות המספקות שירותים של אחסון ועיבוד מאגרי מידע אישי: דוח פיקוח רוחב - ממצאי הליך פיקוח הרוחב בקרב מגזר חברות המספקות שירותים של אחסון ועיבוד מאגרי מידע אישי

העברת מידע בין גופים ציבוריים - רמות עמידה לפי מגזר



ניתן לראות כי קטגוריה זו, במסגרתה נבחן קיומן של ועדות הבוחנות את הצורך במידע, אי העברת מידע עודף והסמכות להעברה וקבלת מידע מגופים ציבוריים ואליהם, נבדקה עד כה בשני מגזרים בלבד הכוללים גופים ציבוריים המחויבים בהוראות פרק ד' לחוק. במגזר מרפאות בריאות הנפש נמצאה עמידה ברמה גבוהה, כאשר עיקר הפערים שנמצאו ושלא באו לידי ביטוי בציון המשוקלל בקטגוריה זו, נבעו מחוסר ידיעה של הגופים המעבירים מידע בנוגע לחובתם בהקמת ועדה להעברת מידע בין גופים ציבוריים. עמידה גבוהה זו מיוחסת בחלקה לדרישות המוטלות על גופים הפועלים במגזר זה כחלק ממערכת החובות המוטלות על ידי משרד הבריאות והרגולציה הפרטנית הנוגעת למתן שירותים רפואיים.

לעומתם, ברשויות המקומיות נמצאה רמת עמידה בינונית-נמוכה במרבית הגופים. עיקר הליקויים בקריטריון זה נבעו מאי-הקמת ועדה להעברת מידע בין גופים ציבוריים בהתאם לנדרש בתקנות. כמו כן, נמצא כי הרשויות המקומיות אשר נמצאו ברמת עמידה נמוכה ובינונית כלל אינן מנהלות רישום בדבר העברות המידע. בהשוואה למרפאות בריאות הנפש ניכר שהרגולציה וההנחיות הקיימות בקרב הרשויות המקומיות אינן מספקות מענה הולם לתחום העברת מידע בין גופים ציבוריים.

קריטריון זה, המתאר את החובות החלות על גופים ציבוריים, רלוונטי לשני מגזרים בלבד בהם בוצעו פיקוחי הרוחב: מגזר בריאות הנפש ומגזר הרשויות המקומיות. הגופים הציבוריים הפועלים במגזר הראשון קיימו באופן מלא את דרישות החוק והתקנות, ובקרב המגזר השני רק 20% מהרשויות נמצאו ככאלו המקיימות את דרישות הדין במלואם.

פיקוחי מעקב

בסיום הליך פיקוחי הרוחב כאמור, הגופים שבהתנהלותם נתגלו ליקויים הונחו להגיש לרשות בתוך זמן קצוב מסמך המפרט את הליקויים אשר תוקנו, והתחייבות חתומה בידי נושא משרה בכיר בארגון לתיקון יתר הליקויים על פי תכנית עבודה מסודרת של הארגון הכוללת לוחות זמנים לביצוע.

בטיפול בתיקון הליקויים נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בקריטריונים הבאים: עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, בקרה ארגונית וממשל תאגידי והעברת מידע בין גופים ציבוריים.

מדי שנה, מבצעת הרשות 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.

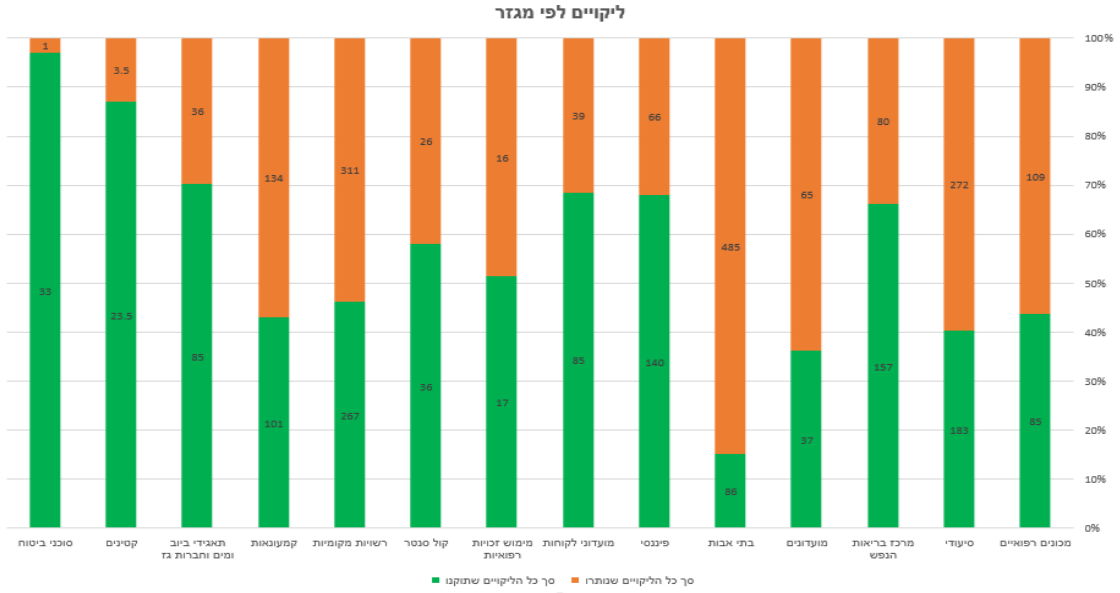
ביחס לגופים שיימצא כי לא מילאו אחר ההנחיה לתיקון ליקויים, רשאית הרשות להטיל סנקציות נוספות העומדות לרשותה מכוח החוק.

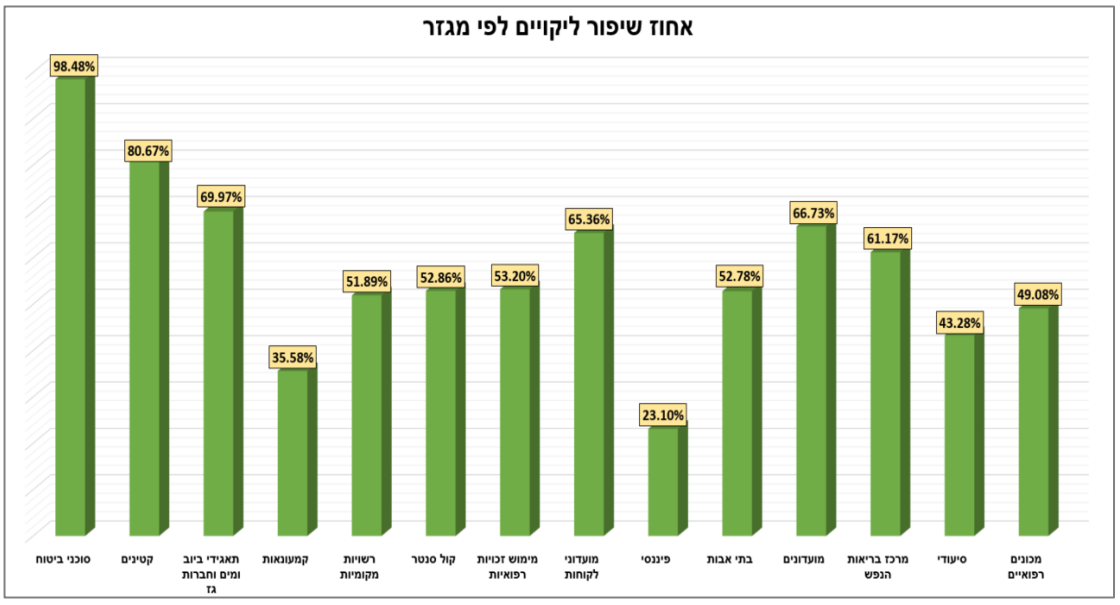
פיקוחי המעקב שמבוצעים במהלך השנים מעידים באופן חד משמעי על כך כי עצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה עצמית באופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרוחב.

שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב לפי מגזרים

חלק מהליקויים דורשים תכנון רב שנתי או היערכות ארוכה להטמעת התיקונים בכלל מאגרי הגופים, בהתאם לסדרי העדיפויות שקבעה הרשות. משכך, בעת פיקוח המעקב בוחנת הרשות את אופן התקדמות תיקון הליקויים אצל הגופים ואת העמידה בלוחות הזמנים שהגדירו ליישום התכנית ותיקון יתרת הליקויים שטרם תוקנו.

הגרפים שלהלן מציגים כאמור את היקף הליקויים שתוקנו ואת יתרת הליקויים שטרם תוקנו הן בהיבט של מספר הליקויים והן בהיבט של אחוזי השיפור שנמדדו בעת ביצוע פיקוח המעקב. ניתן לראות כי בעת עריכת ביקורת המעקב, מרבית המגזרים תיקנו מספר ליקויים משמעותי מתוך כלל הליקויים שנמצאו בפיקוח הרוחב הראשוני, כאשר על הגופים לעדכן את הרשות בדבר לוחות הזמנים וסיום תיקון יתר הליקויים. **מממצאי פיקוחי המעקב עולה כי ממוצע תיקון הליקויים של 14 המגזרים, עומד על 57.44%, מתוכם ב- 6 מגזרים שיעורי התיקון היו מעל הממוצע.**





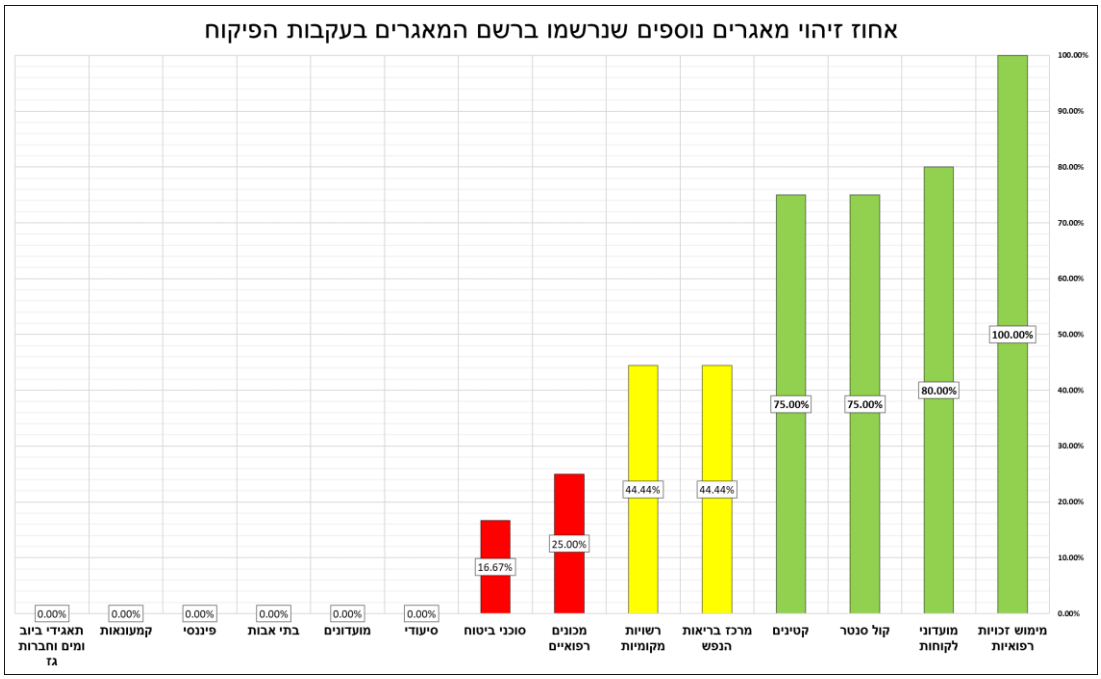
זיהוי ורישום מאגרים בעקבות פיקוח הרוחב

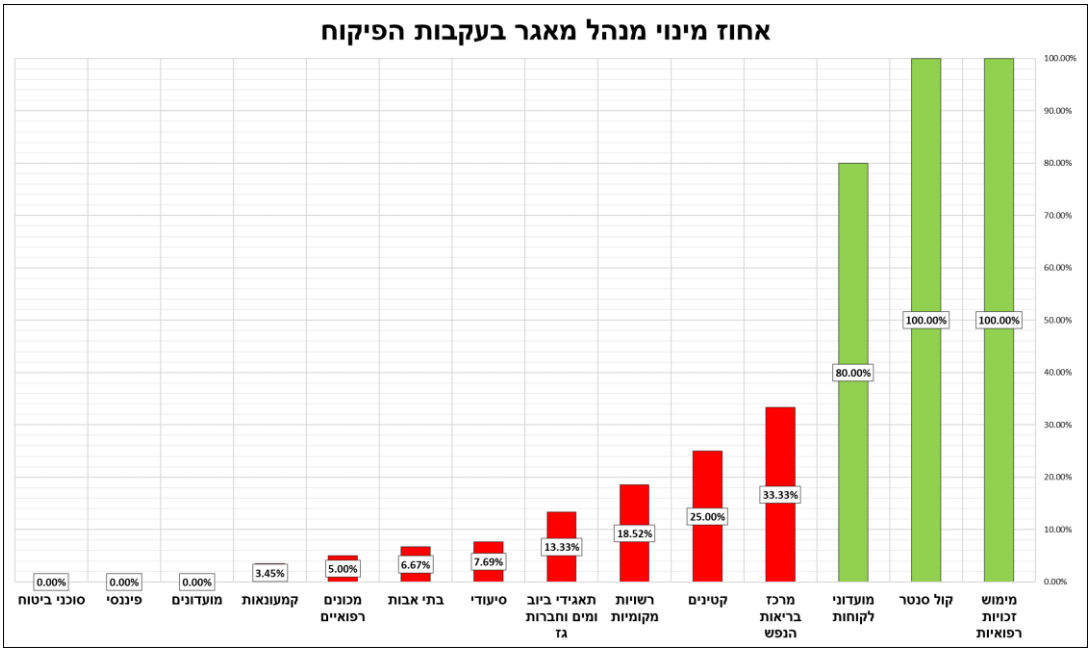
בהתאם לקריטריון הבקרה הארגונית וניהול מאגרי מידע, הגופים המפוקחים המנהלים מאגרי מידע הכוללים אפיון של נושאי המידע, נדרשים על פי חוק לבצע מיפוי לכל מאגרי המידע הקיימים אצלם. על בסיס מיפוי זה, נדרשים הגופים לרשום מאגרי מידע החייבים ברישום ואינם רשומים, או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע. כמו כן, נדרשים הגופים לעדכן כי מינו כדין את הגורמים הנדרשים בחוק ובתקנות, לרבות עדכון פרטי מנהל המאגר בפנקס המאגרים, ככל שמונה כזה.

בחינת קריטריון זה העלתה כי פעילות פיקוח הרוחב הניעה את הגופים לבצע מיפוי באמור ולזהות מאגרי מידע, לרבות מאגרים בעלי רגישות גבוהה שלא נוהלו בהתאם להוראות הדין. במסגרת זו, פעלו הגופים לרישום המאגרים בפנקס המאגרים ולמינוי מנהל המאגר בהתאם.

הגרף שלהלן מציג את אחוז הגופים שבמסגרת הליך פיקוח הרוחב זיהו כי ברשותם מאגרים באמור, ופעלו לרישומם בפנקס המאגרים. יובהר, כי הנתונים שלהלן מתארים את אחוז הגופים שנדרשו לרישום באמור, וביצעו זאת נכון למועד פיקוח המעקב. מממצאי פיקוח המעקב עולה כי ב-4 מגזרים בוצע איתור וזיהוי מאגרים בשיעור גבוה (75%-100%), בשני מגזרים זיהוי בשיעור בינוני (33%-75%), וב-2 מגזרים זיהוי בשיעור נמוך באופן יחסי, או שהגופים כלל לא נדרשו לזיהוי ורישום (10%-33%).

בהתאם לממצאי פיקוח המעקב, בכל הנוגע למינוי מנהל מאגר, ממוצע המינויים שבוצעו בעקבות פיקוח הרוחב עמד על 28%. מבין 11 המגזרים, ב-3 מגזרים מונו מנהלי מאגר בעקבות פיקוח הרוחב (בשיעור גבוה של בין 80%-100%), וב-8 מגזרים שיעור המינוי היה נמוך יחסית (3%-33%).

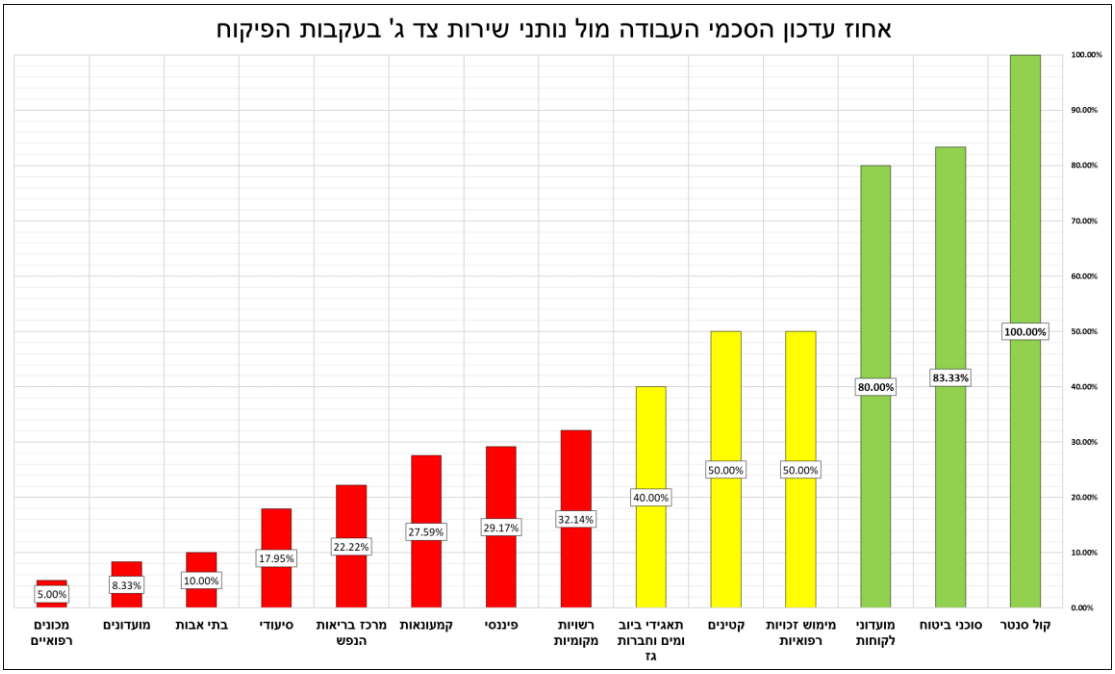




עדכון הסכמים מול גורמי מיקור חוץ בעקבות פיקוח הרוחב

בהתאם לקריטריון הבוחן את אופן עיבוד המידע האישי במיקור חוץ, נדרשו הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות, ולוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר. בהסכם יש לקבוע במפורש את כל ההוראות המתחייבות על פי תקנה 15(א)(2) לתקנות אבטחת מידע, ולנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות, כנדרש בתקנה.

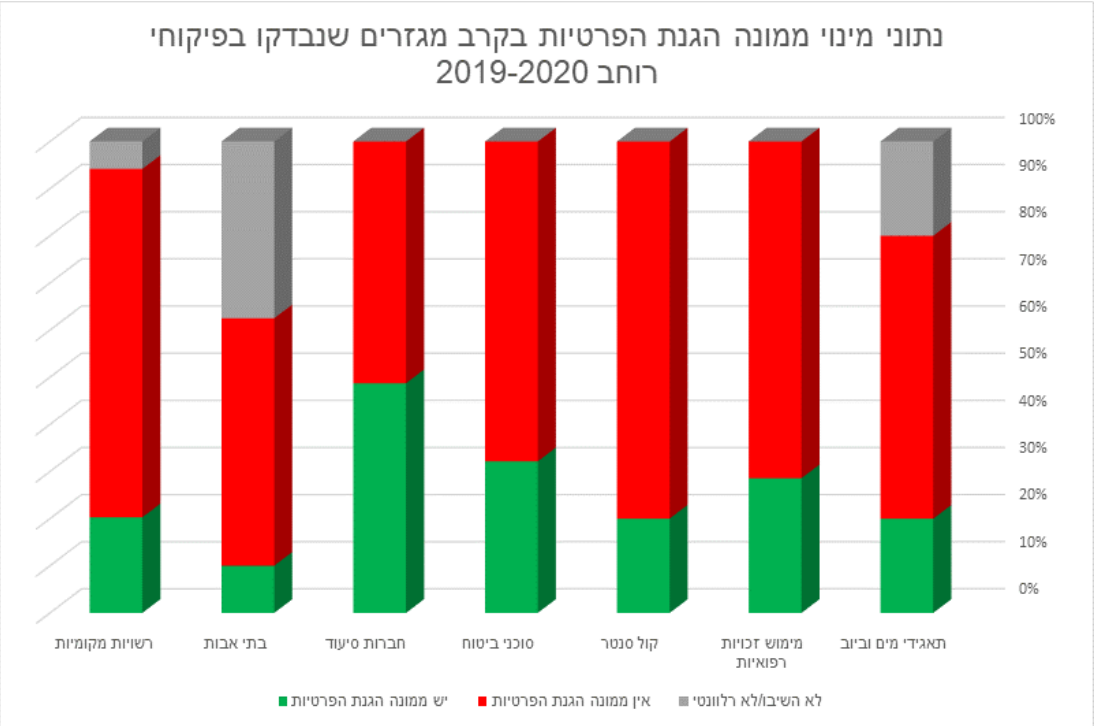
הגרף שלהלן מציג את שיעור עדכוני ההסכמים מול נותני שירותי עיבוד מידע במיקור חוץ בהתאם לדרישות תקנה 15. מן הממצאים ניתן לראות כי כלל המגזרים שיפרו ויישמו את חובתם הודות להליך הפיקוח ועדכנו את ההסכמים. במגזר אחד הצוותים עדכנו במלואם את ההסכמים (100%). בשני מגזרים שיעור גבוה מההסכמים עודכנו (80-83%). ב-3 מגזרים שיעור בינוני מההסכמים עודכנו (40-50%). ב-8 מגזרים עודכן שיעור נמוך בלבד מההסכמים (5-32%).

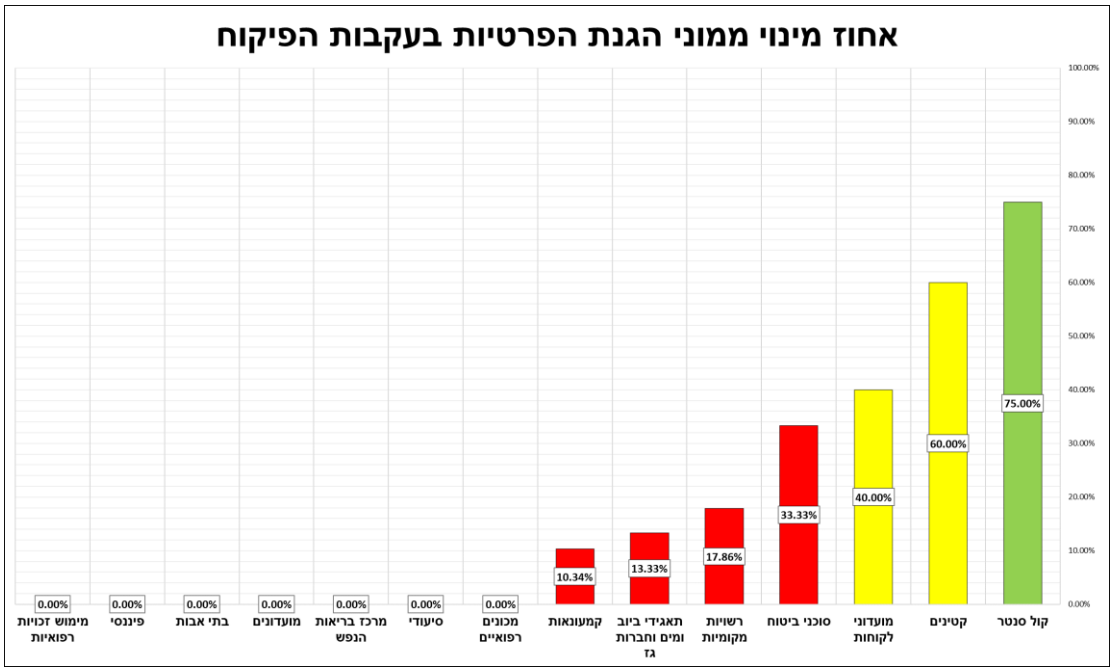


מינוי ממונה הגנת הפרטיות שדווחו בעת פיקוח הרוחב לשנים 2019-2020

במסגרת הליך פיקוח הרוחב, נשאלו הגופים המפוקחים, כשאלת רשות, האם יש בארגון ממונה הגנת הפרטיות, תוך ציון שאין כיום חובה בדין למינוי ממונה כאמור. בהתבסס על ממצאי 203 גופים מפוקחים ב-7 מגזרים שונים, בין השנים 2019-2020, ניתן לראות עלייה במינוי ממונה הגנת הפרטיות, ככל הנראה כתוצאה מקיום הליך הפיקוח[11]

[11] בשנת 2020 פרסמה הרשות להערות הציבור מסמך מקיף בנוגע למינוי ממונה הגנת הפרטיות בארגון ותפקידיו. בינואר 2022 פורסם המסמך בגרסתו הסופית. המסמך כולל המלצות פרקטיות לארגונים וחברות מכלל מגזרי המשק, ומתייחס בהרחבה למרכיבי התפקיד, סמכויותיו של הממונה, הידע וההכשרה הנדרשים, היחס בינו לבין בעלי תפקידים אחרים בארגון ועוד. במקביל, פרסמה הרשות גם ערכת הדרכה בנושא. - מינוי ממונה הגנה על הפרטיות - מדריך


נתוני מינוי ממונה הגנת הפרטיות בקרב מגזרים שנבדקו בפיקוחי רוחב 2019-2020
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
רשויות מקומיות
בתי אבות
חברות סיעוד
סוכני ביטוח
קול סנטר
מימוש זכויות רפואיות
תאגידי מים וביוב
יש ממונה הגנת הפרטיות
אין ממונה הגנת הפרטיות
לא השיבו/לא רלוונטי


אחוז מינוי ממוני הגנת הפרטיות בעקבות הפיקוח
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
0.00%
0.00%
0.00%
0.00%
0.00%
0.00%
10.34%
13.33%
17.86%
33.33%
40.00%
60.00%
75.00%
מימוש זכויות רפואיות
פיננסי
בתי אבות
מועדונים
מרכז בריאות הנפש
סיעודי
מכונים רפואיים
קמעונאות
תאגידי ביוב ומים וחברות גז
רשויות מקומיות
סוכני ביטוח
מועדוני לקוחות
קטינים
קול סנטר

סיכום

ממצאי הדוחות שפורסמו על ידי הרשות מלמדים על סיכונים רבים לפרטיות נושאי המידע בקרב המגזרים השונים הנכללים בהליך פיקוח הרוחב. הגופים השונים במגזרים אלה מנהלים מידע רב, מזוהה ורגיש, לצד קשר אינטראקטיבי עם נושאי המידע במישרין ובאמצעות ספקי מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות החוק והתקנות, שקיפות מול נושא המידע, ומילוי החובות החלות מכוח פרק הדיווח הישיר ושירותי הדיווח הישיר בחוק.

מממצאי הליך פיקוח הרוחב במגזרים השונים, עולה כי גופים רבים אינם מקפידים דיים ליידע את ציבור נושאי המידע בדבר זכויותיו על פי החוק, הכוללות בין היתר את החובה להציג את מקור המידע, הזכות לעיין במידע והזכות לתקן את המידע אודותיך הכלול במאגר.

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל המפוקחים במגזרים השונים תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית מסודרת לתיקונם.

פיקוח הרוחב העלה כי מרבית הליקויים זוהו בקריטריונים של מיקור חוץ, אבטחת מידע, ובקרה ארגונית. עם זאת, מפיקוחי מעקב תיקון הליקויים עולה, כי קיים שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות, כתוצאה מהליך פיקוח הרוחב.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בהתאם לסקרי הסיכונים אותם היא מבצעת, בקרב בעלים ומחזיקים במאגרי מידע אישי באמצעות הליך פיקוחי הרוחב, לרבות בדרך של פיקוחי מעקב לבחינת אופן תיקון הליקויים ויישום ההנחיות על-ידי הגופים שנדרשו לכך במסגרת ההליך, וכן תמשיך ותבחן את אופן השיפור ביישום הוראות החוק והתקנות בקרב המגזרים אותם בדקה בעבר. הרשות תמשיך ותפרסם דוחות מגזריים לציבור הכוללים את ממצאי פיקוחי הרוחב והמלצות לתיקון ליקויים לשם הגברת עמידת הגופים הפועלים במגזרים אלו בהוראות החוק והתקנות ועל מנת לחזק את ההגנה על זכות הציבור לפרטיות.