דוח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר הפלסטיקה והכירורגיה הקוסמטית



אדר ב' תשפ"ד

מרץ 2024

תוכן עניינים

1.תקציר מנהלים..... 2

1.1.מגזר חברות פלסטיקה וכירורגיה קוסמטית..... 2

1.2.תהליך העבודה..... 3

1.3.ליקויים, מסקנות והמלצות עיקריות..... 3

2. חברות פלסטיקה וכירורגיה קוסמטית - תמונת מצב 6

2.1.כללי..... 6

2.2.רקע על המגזר..... 6

2.3.תהליך עבודה..... 7

2.4.הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו..... 8

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

3.1.בקרה ארגונית..... 10

3.2.ניהול מאגרי מידע ועיבוד מידע אישי במיקור חוץ..... 12

3.3.אבטחת מידע..... 14

4. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב..... 16

5.סיכום..... 17

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 (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, לאיתור כשלים ענפיים וכלל-משקיים הדורשים התייחסות מוגברת של הרגולטור, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר חברות פלסטיקה וכירורגיה קוסמטית

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר פלסטיקה וכירורגיה קוסמטית בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים. זאת, בשל מאפייניו הייחודיים של מגזר זה הבאים לידי ביטוי במספר היבטים:

- **איסוף והחזקה של מידע רגיש ובכלל זה מידע רפואי אודות לקוחות הגופים במגזר.**
- **הגופים במגזר זה עושים שימוש במערכת דיוור ישיר ושירותי דיוור ישיר, ובמסגרת זאת עליהם לקיים חובות פרטניות של שקיפות בכל פנייה כאמור לנושא המידע.**

מאפיין נוסף של מגזר זה מתייחס למבנה ופעילות גופים אלו. גופים אלה מחזיקים מאגרי מידע המכילים מידע רגיש בהיקפים עצומים ומנוהלים לרוב בידי עצמאיים או עוסקים שאינם מאוגדים תחת המעטפת של חברה גדולה. עקב כך, ברוב המקרים, אין בגופים אלה בעלי תפקידים ייעודיים לטיפול בנושא הגנת הפרטיות, דבר אשר מקשה על שמירת פרטיותם של לקוחותיהם.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותם גופים לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית ועמידה בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר.

נוכח כל אלה הרשות להגנת הפרטיות הגדירה מגזר זה כיעד פיקוח רוחב משמעותי.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל- 27 גופים המעניקים שירות בנושא פלסטיקה וכירורגיה קוסמטית המנהלים מאגרי מידע, כאשר בחלק מן המקרים נדרשו הגופים בהמשך לספק מידע, מסמכים והבהרות נוספות לרשות. שאלוני הביקורת בחנו מספר קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית, ניהול מאגרי מידע לרבות השימוש בגורם חיצוני, ואבטחת מידע. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. 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.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר פלסטיקה וכירורגיה קוסמטית נמצאה רמת עמידה **נמוכה** בכל הקשור **באבטחת מידע**, ומאידך רמת עמידה גבוהה בכל הקשור **בניהול מאגרי מידע**. נדגיש כי נמצאו ליקויים שחוזרים על עצמם במספר רב של גופים בנושא **שימוש במיקור חוץ**. בכל הקשור **בבקרה ארגונית** נמצאה רמת עמידה בינונית-נמוכה.

נוכח הממצאים שעלו מהליך פיקוח הרוחב, קיבלו 21 מתוך 21 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

ממצאי הליך פיקוח רוחב
בקרב מגזר הפלסטיקה והכירורגיה הקוסמטית

דו"ח פיקוח רוחב 2020-2021

אתגרים ומאפיינים ייחודיים של מגזר חברות פלסטיקה וכירורגיה קוסמטית

הגופים במגזר זה עושים שימוש במערכת דיוור ישיר ושירותי דיוור ישיר, ובמסגרת זאת עליהם לקיים קיום חובות פרטניות של שקיפות בכל פנייה כאמור לנושא המידע

הגופים במגזר זה מנהלים מתוקף עיסוקם נתונים רגישים - מאגרי מידע הכוללים מידע רגיש ובכלל זה מידע רפואירגיש אודות מטופלים.

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

התהליך שבוצע במספרים

27 שאלונים שהופצו

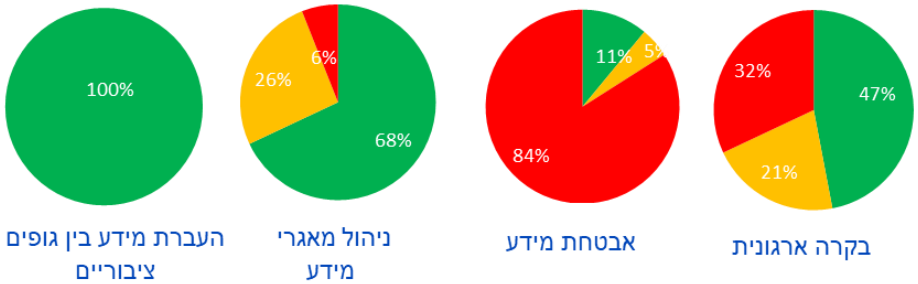
3 גופים שנדרשו להשלמת ידיעות ומסמכים

21 גופים שהשתתפו בפועל בהליך הפיקוח (למעט גופים שהוסרו מההליך או הועברו להמשך טיפול אכיפתי)

21 הנחיות לתיקון ליקויים

ממצאים – ליקויים מרכזיים:

ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר



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 כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר בהתאם להוראות ההסכם 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 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 אחר הכפוף ישירות למנהל המאגר.
- יש לערוך ביקורות בנושא אבטחת מידע והגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.



- 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 אבטחה 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 בנקיטת 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, ולפעול לתיקון הליקויים שהתגלו במסגרת המבדקים.

2. פלסטיקה וכירורגיה קוסמטית - תמונת מצב

2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים אוקטובר 2020 למאי 2021 במגזר הפלסטיקה והכירורגיה הקוסמטית.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר הפלסטיקה והכירורגיה הקוסמטית בישראל כאחד מיעדי פיקוח הרוחב המשמעותיים וזאת בשל מאפייניו הייחודיים של מגזר זה הכוללים איסוף והחזקה של מידע רפואי, סודי ורגיש אודות לקוחות הגופים וכן השימוש שעושים גופים במגזר זה במערכת דיוור ישיר ושירותי דיוור ישיר.

גופים אלו, שהם בעליהם של מאגרי מידע גדולים ורגישים מאוד, מנוהלים לרוב בידי עצמאיים ובעלי עסקים שאינם מאוגדים תחת המעטפת של חברה גדולה. לכן, ברוב הגופים לא מוקצים בעלי תפקידים ייחודיים לטיפול בנושא הגנת הפרטיות, דבר אשר יוצר קושי בשמירה על פרטיותם של לקוחותיהם.

ניהול המאגרים בהתייחס למאפייניו הייחודיים של המגזר מחייב את אותם גופים לעמוד בדרישות החוק והתקנות ביתר שאת, לרבות קיום חובות אבטחת המידע, קיום בקרה ארגונית ועמידה בהוראות החוק בכל הנוגע לדיוור ישיר ולשירותי דיוור ישיר.

2.3. תהליך העבודה

במטרה לפעול באופן המיטבי ביותר למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, נוקטת הרשות להגנת הפרטיות בגישה מבוססת סיכון הבוחנת כל העת את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש לפעולותיה על המשק. על מנת לעמוד במכלול האתגרים העומדים לפתחה, הרשות פועלת על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות של הרשות ומאפשר לעסוק, בין היתר, בתחומים בהם ישנה השפעה רוחבית על מגזרים שונים, הכוללים מספר רב של משתמשים 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. התכנית נבנית בהתחשב בקריטריונים הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

הליך הפיקוח בוצע ב-27 גופים שהינם חלק ממגזר הפלסטיקה והכירורגיה הקוסמטית. בסופו של יום, השיבו לשאלוני הפיקוח 21 גופים שנבחרו על ידי הרשות, בניכוי גופים אשר הועברו להמשך טיפול אכיפתי או שסיימו פעילותם, שינו פעילות, דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, ולאחר איחוד גופים אשר השיבו מענה מאוחד בשל פעילות עסקית מאוחדת או ניהול שימוש במאגר או תשתית טכנולוגית משותפת.

בסיום ההליך, מתוך 21 הגופים המפוקחים, נמצאו ב-21 גופים ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את אותם גופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, ביצעה הרשות ביקורת חוזרת מדגמית לבחינת השלמת התיקונים ב 16 גופים.

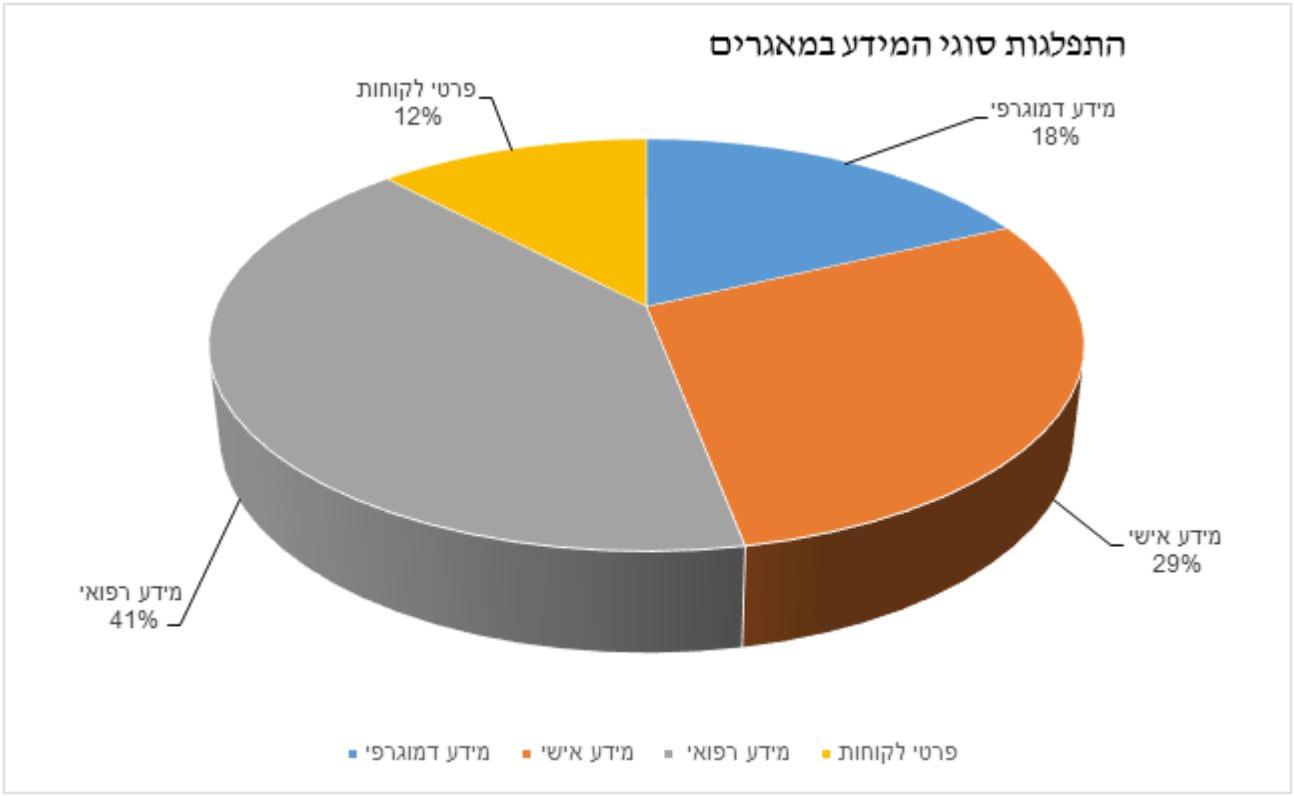
2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו

במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לקריטריונים שונים ובהם:

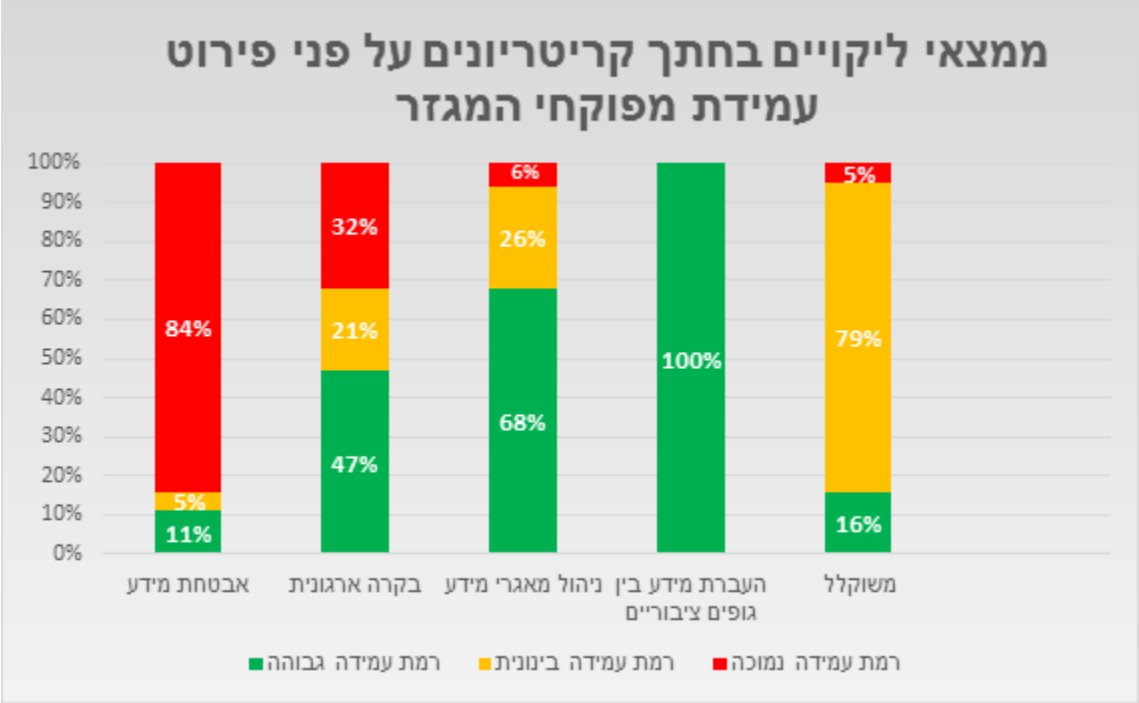


רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הגופים במגזר הפלסטיקה והכירורגיה הקוסמטית, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרת ההליך:

- עמידה של בין 80% - 100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;
- עמידה של בין 50% - 80% מוגדרת כרמת עמידה בינונית או חלקית;
- עמידה של מתחת ל-50% מוגדרת כרמת עמידה נמוכה.

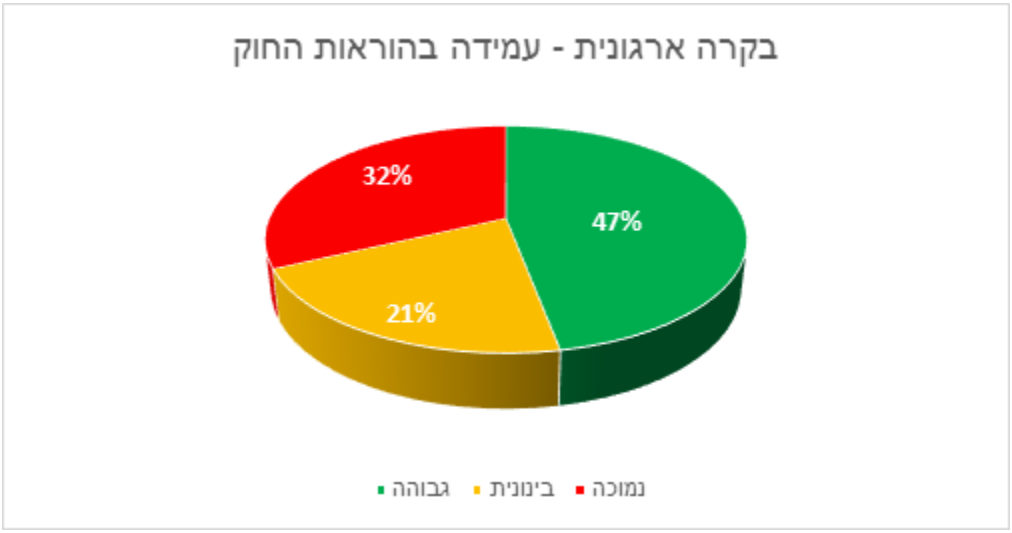


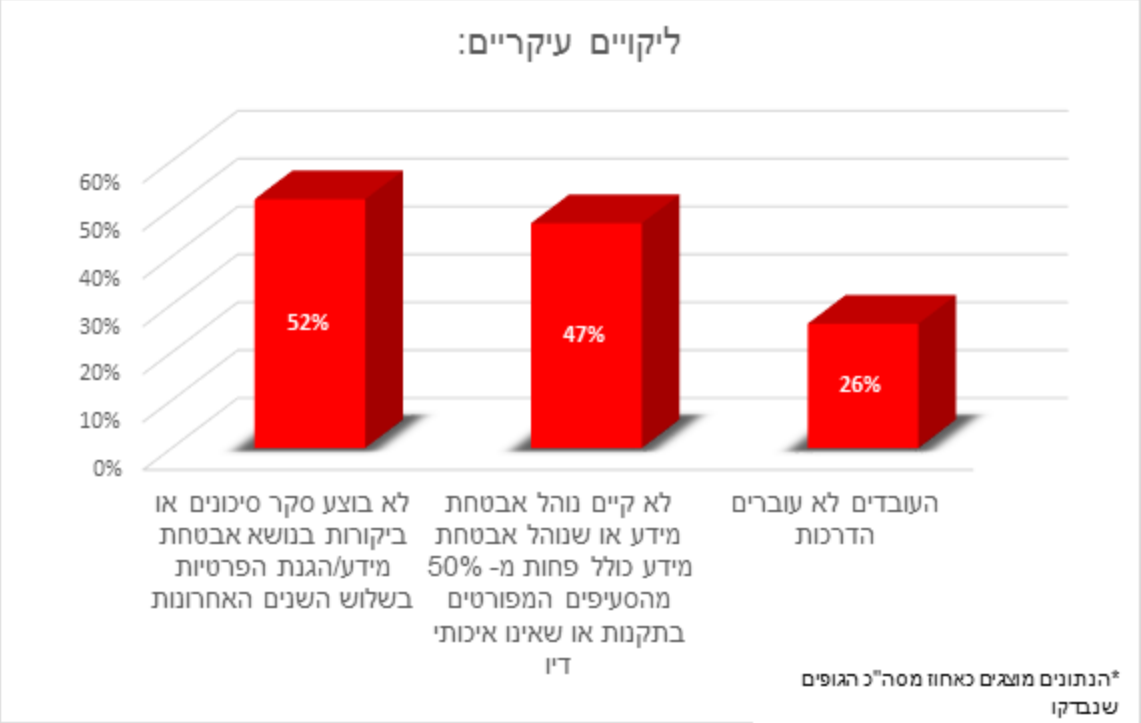
3. ממצאים – ליקויים מרכזיים לפי קריטריונים במבט השוואתי והמלצות:



3.1. בקרה ארגונית

ממצאים:





המלצות:

נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים המפוקחים, בין היתר, לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאות כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע ככל שהדבר נדרש לפי הוראות סעיף 17ב לחוק, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות אבטחת מידע.

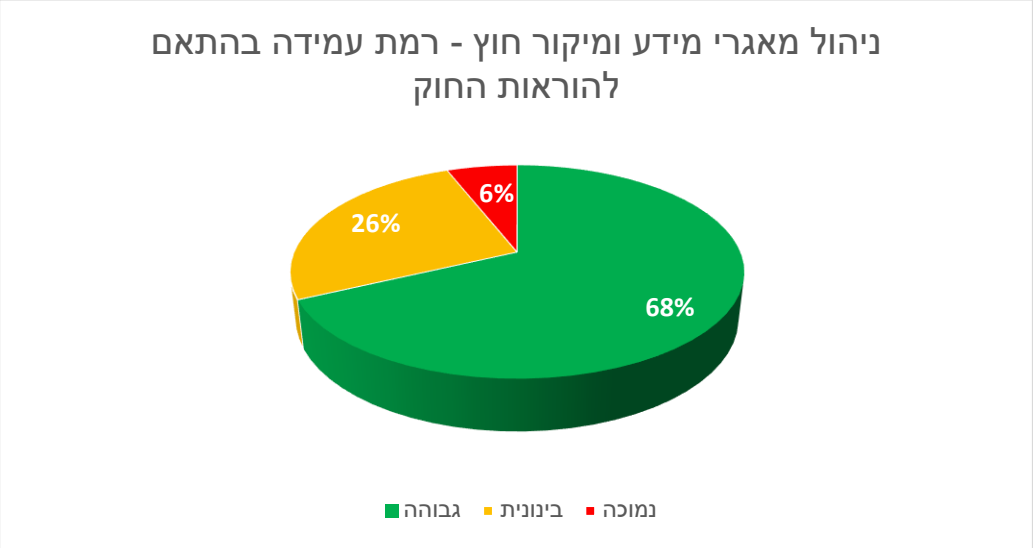
כמו כן, על הגופים המפוקחים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון: אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשה גישה, ניהול סיכונים, התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות אבטחת מידע (תקנה 4).

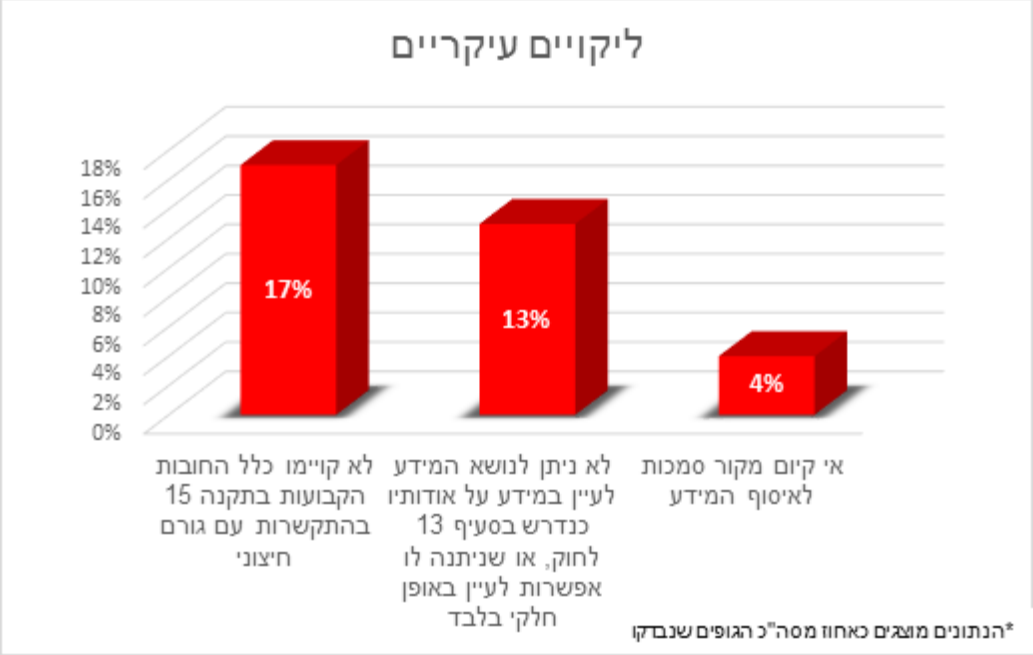
כמו כן, ככל שמדובר בגוף שחלה עליו רמת האבטחה הגבוהה וכזה הוא חייב במבדקי חדירות, עליו לוודא כי בוצעו מבדקי חדירות וכי הם עומדים בדרישות תקנות אבטחת מידע (תקנה 16).

בנוסף, בהתאם לנדרש בתקנה 7 לתקנות אבטחת מידע, על הגופים המפוקחים לערוך הליך מיון (בדיקת התאמה) לעובדים חדשים או לכל גורם אחר שמקבל גישה למאגר או למערכת הכוללת מספר מאגרים.

3.2. ניהול מאגרי מידע ומיקור חוץ

ממצאים:





המלצות:

מכוח החובה המוטלת על פי החוק על הגופים המפוקחים המנהלים מאגרי מידע על לקוחותיהם, הכוללים אפיון של נושאי המידע לרבות מידע עליהם, נדרשים גופים אלה לבצע מיפוי של כל מאגרי המידע הקיימים אצלם, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים, או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע. בנוסף, נדרשים הגופים המפוקחים לוודא קיום התאמה בין זהות מנהל המאגר במסמכי החברה לבין מנהל המאגר הרשום אצל רשם מאגרי המידע.

על הגופים המפוקחים לקבל את הסכמת נושא המידע כנדרש בחוק עבור איסוף מידע ושמירת פרטיו במאגרי הארגון. זאת, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

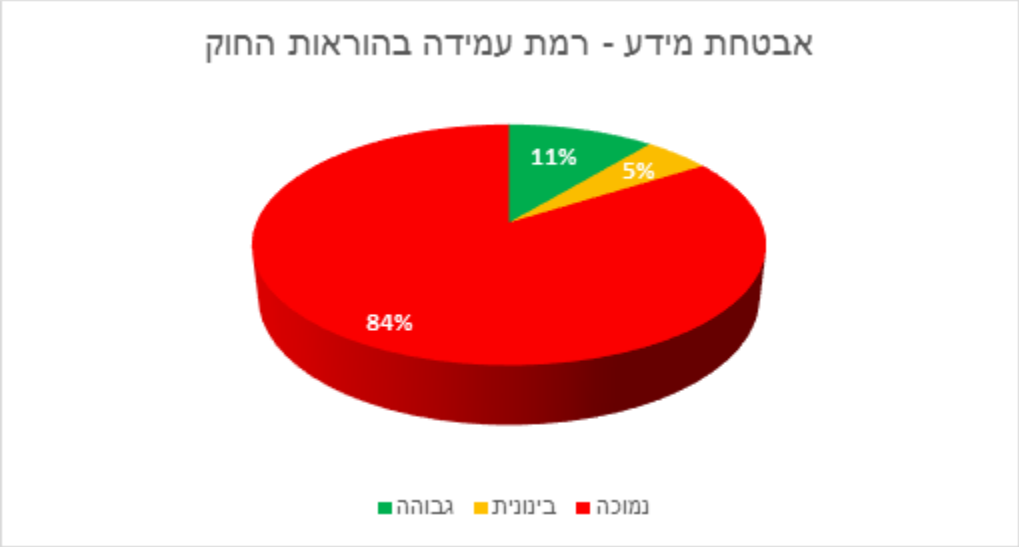
בנוסף, על הגופים המפוקחים להקפיד לאפשר לנושאי המידע לעיין במידע על אודותיהם, המוחזק במאגר מידע בהתאם לבקשת בעל המאגר, ובפניה ישירה של נושא המידע למסור אם הם מחזיקים מידע עליו וכן את שם בעל מאגר המידע ואת מענו, בהתאם לסעיף 13 לחוק. לעניין זה, יודגש כי זכות העיון חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות, תכתובות צ'ט, שיחות המצולמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי. כמו כן, יש להקפיד לאפשר לנושאי המידע לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע, בהתאם לסעיף 14 לחוק.

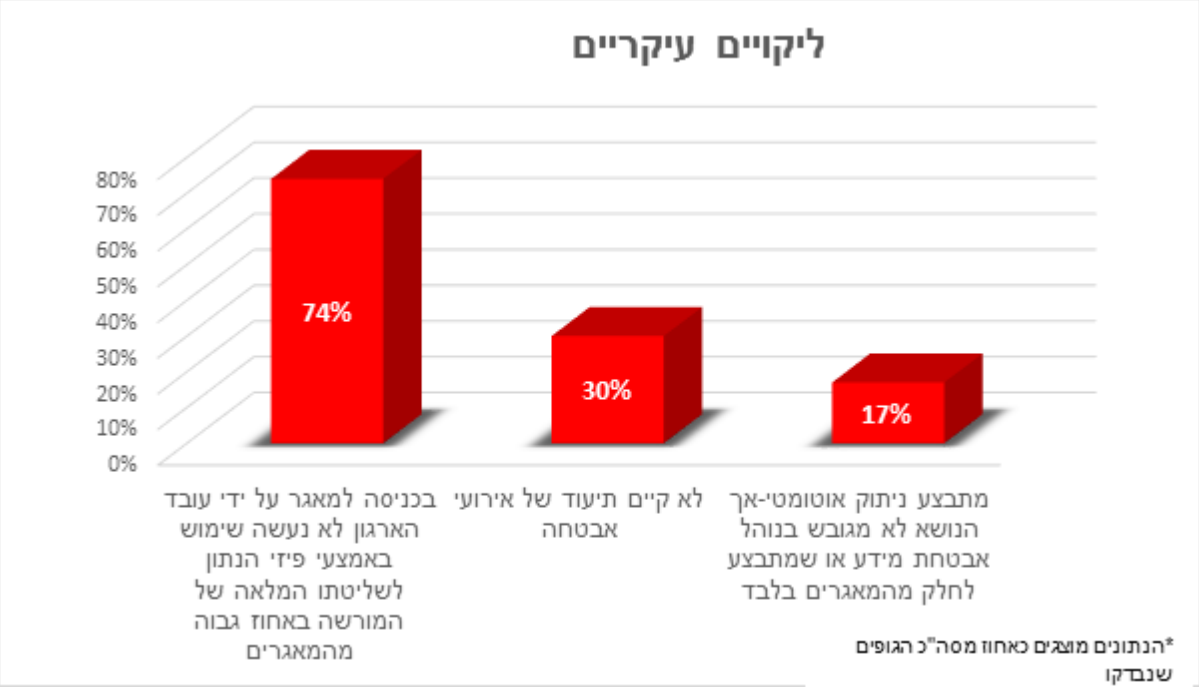
בעת שימוש בשירותי מיקור חוץ נדרש בעל המאגר לפעול בהתאם להוראות תקנה 15 לתקנות, וכן ליישם את הוראות הנחיית הרשות להגנת הפרטיות מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי.[1] בפרט, יש לפעול לעיגון ההתייחסות לחובותיו ואחריותו של הספק במסמך ההתקשרות, בהתאם להוראות התקנות, ולוודא כי כל גורם 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.

[1] הנחיית רשם מאגרי המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי". ההנחיה זמינה כאן

3.3. אבטחת מידע

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

המלצות:

נוכח הליקויים הרוחביים שנמצאו במגזר זה בנושא ניהול ההרשאות, על הגופים המפוקחים להטמיע מנגנוני הרשאות במאגרי המידע של הארגון המבוססים על הצורך לדעת (בעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות), וזאת בהתאם לתקנות 8 ו -9 (א) לתקנות אבטחת מידע. מנגנוני הרשאות אלו יבטיחו הפרדת סמכויות ויבטיחו אפשרות גישה לנתוני המאגר אך ורק במידה הנדרשת לביצוע התפקיד של העובדים בעלי הגישה למידע.

בנוסף, על הגופים המפוקחים לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע. כמו כן, עליהם לוודא שבכניסה לאתר מאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה על פי תקנות אבטחת מידע (תקנה 9(ב)(2)).

במאגרים בעלי רמת אבטחה גבוהה, יש לבצע מבדקי חדירות אחת ל- 18 חודשים, בהתאם לתקנה 5 (ד) לתקנות אבטחת מידע.

כמו כן, נוכח הליקויים שנמצאו בנוגע לשימוש בהתקנים ניידים במגזר זה, מוצע כי הגורמים הרלוונטיים בגופים המפוקחים יבחנו את הצורך בחיבור התקנים ניידים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – יש להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.

על הגופים ליישם מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר ושמירת מעקב אודות נתונים כגון: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

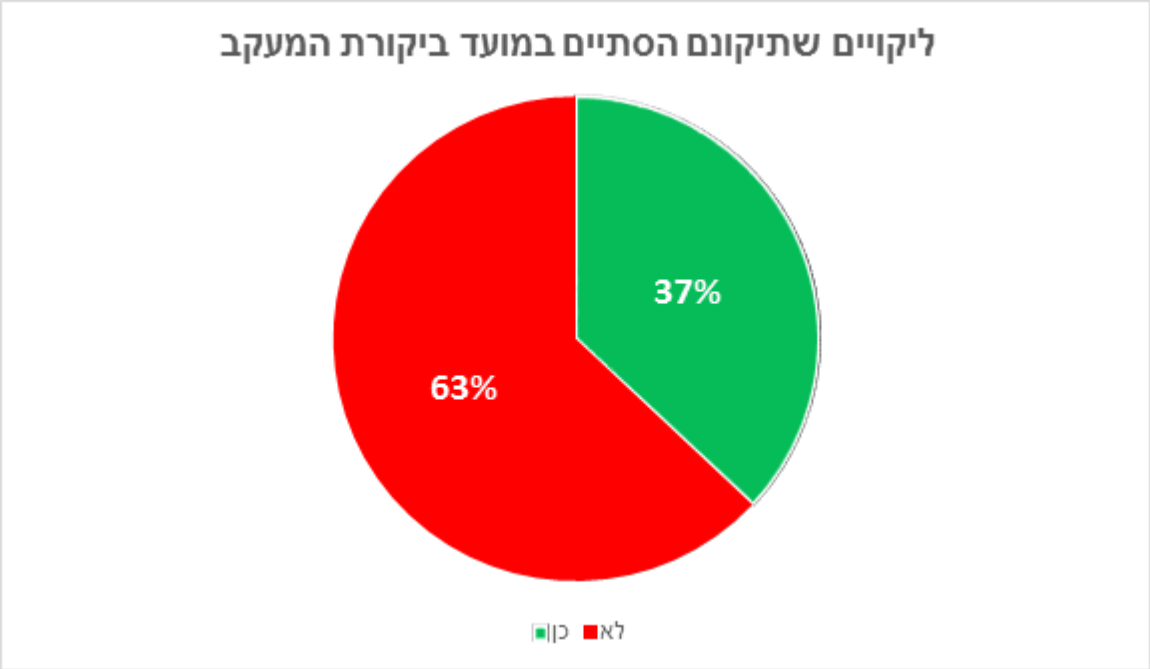
בנוסף, יש לקבוע נהלים ולפעול להטמעת תהליכי גיבוי ללוג נתוני האבטחה בכל המאגרים באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי בהתאם לתקנות.

4. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2021, נערך מעקב מדגמי לתיקון ליקויים במגזר הפלסטיקה והכירורגיה הקוסמטית, 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, בוצעו ע"י הרשות להגנת הפרטיות, פיקוחי מעקב על הגופים 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 בוחנה 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 70% מהגופים במגזר הפלסטיקה והכירורגיה הקוסמטית שקיבלו הנחיות לתיקון ליקויים, נמצא כי במועד הבדיקה הגופים נמצאו בהליך של שיפור ותיקון רמת העמידה בחוק ובתקנות הגנת הפרטיות, כאשר 37% מתוכם השלימו את תיקון 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.



5. סיכום

בפעילות מגזר הפלסטיקה והכירורגיה הקוסמטית קיימים סיכונים לא מעטים לפרטיות, אשר נובעים מניהול ואחזקת מידע רב, מזוהה ורגיש, וניהול קשר ישיר עם לקוחות הגופים באמצעות הגופים עצמם ובאמצעות שימוש במיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות אבטחת מידע, שקיפות מול הלקוח, ומילוי החובות החלות מכוח פרק הדיוור הישיר ובחוק הגנת הפרטיות.

הליך פיקוח הרוחב במגזר הפלסטיקה והכירורגיה הקוסמטית העלה ממצאים מדאיגים המצביעים על ליקויים בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע, בקרה ארגונית וממשל תאגידי, וניהול מאגרי מידע, **כאשר נמצאו פערים רבים בעמידה בהוראות החוק בכל הנוגע לקטגוריית אבטחת מידע.**

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 הפלסטיקה והכירורגיה הקוסמטית, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.